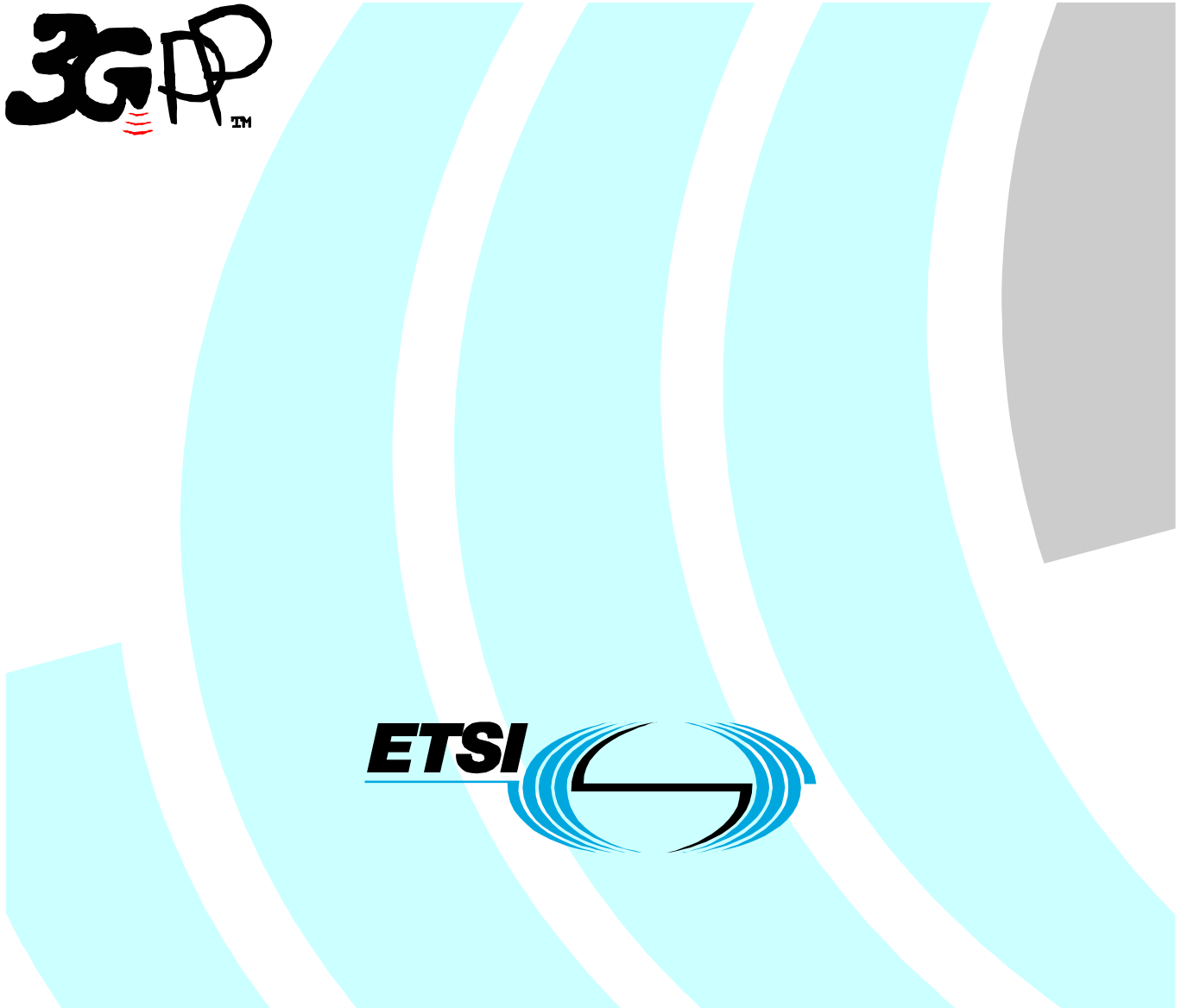
ETSI TS 129 202 V4.1.1 (2002-06)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Signalling System No. 7 (SS7) signalling transport in core network;
Stage 3
(3GPP TS 29.202 version 4.1.1 Release 4)



Reference
RTS/TSGN-0429202v411

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2002.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 6
4 Introduction 6
5 Protocol Architectures 7
5.1 Protocol architecture in the case of MTP-based SS7 signalling transport network 7
5.2 Protocol architecture in the case of IP-based SS7 signalling transport network 7
5.3 Protocol architecture in the case of ATM-based SS7 signalling transport network 7
Annex A (normative): Internet Draft: SS7 MTP3-User Adaption Layer (M3UA) 9
Annex B (informative): Change history 173
History 174

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the possible protocol architectures for transport of SS7 signalling protocols in Core Network.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

2.1 Normative references

[1] 3GPP TR 21.905: "3G Vocabulary"

[2] ITU-T Recommendation Q.701: "Functional description of the message transfer part (MTP) of signalling system No. 7"

[3] ITU-T Recommendation Q.702: "Signalling data link"

[4] ITU-T Recommendation Q.703: "Signalling link"

[5] ITU-T Recommendation Q.704: "Signalling network functions and messages"

[6] ITU-T Recommendation Q.705: "Signalling network structure"

[7] ITU-T Recommendation Q.706: "Message transfer part signalling performance"

[8] RFC 2960: "Stream Control Transmission Protocol"

[9] ITU-T Recommendation G.804: "ATM cell mapping into Plesiochronous Digital Hierarchy (PDH)"

[10] ITU-T Recommendation I.112: "Vocabulary of terms for ISDNs"

[11] ITU-T Recommendation I.361: "B-ISDN ATM layer specification"

[12] ITU-T Recommendation I.363.5: "B-ISDN ATM Adaptation Layer specification: Type 5 AAL"

[13] ITU-T Recommendation Q.2110: "B-ISDN ATM adaptation layer - Service specific connection oriented protocol (SSCOP)"

[14] ITU-T Recommendation Q.2140: "B-ISDN ATM adaptation layer - Service specific coordination function for signalling at the network node interface (SSCF at NNI)"

[15] ITU-T Recommendation Q.2210: "Message transfer part level 3 functions and messages using the services of ITU-T Recommendation Q.2140"

2.2 Informative references

[16] RFC 2719: "Framework Architecture for Signalling Transport"

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAL5	ATM Adaptation Layer type 5
ATM	Asynchronous Transfer Mode
IP	Internet Protocol
MTP	Message Transfer Part
MTP1	Message Transfer Part layer 1
MTP2	Message Transfer Part layer 2
MTP3	Message Transfer Part layer 3
M3UA	MTP3-User Adaptation
PDH	Plesiochronous Digital Hierarchy
SSCF	Service Specific Coordination Function
SSCOP	Service Specific Connection Oriented Protocol
SCCP	Signalling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
TCAP	Transaction Capabilities Application Part

4 Introduction

The Core Network enables the transport of SS7 signalling protocols between two entities by means of different underlying networks (e.g. MTP-based, IP-based or ATM-based).

The transport of SS7 signalling protocol messages of any protocol layer that is identified by the MTP level 3 layer, in SS7 terms, as a user part (MTP3-user) shall be accomplished in accordance with the protocol architecture defined in the following sub-clauses. The list of these protocol layers includes, but is not limited to, Signalling Connection Control Part (SCCP).

The transport of protocols which can be identified as SCCP-users, like for example TCAP, and in turn the transport of TCAP-users like MAP and CAP, shall also be accomplished in accordance with the defined protocol architectures, since their protocol messages are transferred as SCCP payload.

5 Protocol Architectures

5.1 Protocol architecture in the case of MTP-based SS7 signalling transport network

The transport of an MTP3-user signalling messages shall be accomplished in accordance with the relevant ITU-T Recommendations [2], [3], [4], [5], [6], [7].

The protocol architecture applicable in the case of MTP-based SS7 signalling transport network is shown in Figure 5.1/1

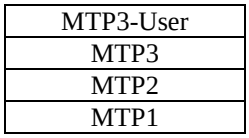


Figure 5.1/1: Protocol architecture in the case of MTP-based SS7 signalling transport network

5.2 Protocol architecture in the case of IP-based SS7 signalling transport network

The transport of an MTP3-user signalling messages shall be accomplished in accordance with the architecture defined by the "Framework Architecture for Signalling Transport" [16], by "Stream Control Transmission Protocol"[8] and by the IETF document available in Annex A

The protocol architecture applicable in the case of IP-based SS7 signalling transport network is shown in Figure 5.2/1

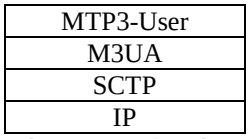


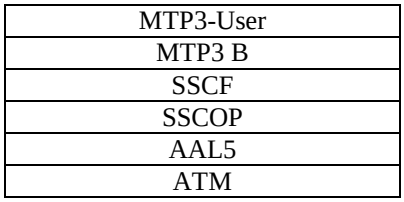
Figure 5.2/1: Protocol architecture in the case of IP-based SS7 signalling transport network

5.3 Protocol architecture in the case of ATM-based SS7 signalling transport network

The transport of an MTP3-user signalling messages shall be accomplished in accordance with the relevant ITU-T Recommendations [9], [10], [11], [12], [13], [14], [15]

The protocol architectures applicable in the case of ATM-based SS7 signalling transport network are shown in Figure 5.3/1.

ATM over SDH



ATM over PDH

MTP3-User
MTP3 B
SSCF
SSCOP
AAL5
G.804

Figure 5.3/1: Protocol architectures in the case of ATM-based SS7 signalling transport network

Annex A (normative):
Internet Draft: SS7 MTP3-User Adaption Layer (M3UA)

The document included in this Annex is the latest available Internet-Draft at the time of writing. When the IETF issues the RFC to this Internet-Draft then a change request will be provided to replace the text in Annex A with a reference in section 2

Network Working Group Greg Sidebottom (Editor)
INTERNET-DRAFT Guy Mousseau
Nortel Networks
Lyndon Ong
Ciena
Ian Rytina
Ericsson
Hanns-Juergen Schwarzbauer
Siemens
Klaus Gradischnig
Neustar
Ken Morneault
Cisco
Mallesh Kalla
Telcordia
Normand Glaude
Performance Technologies

Expires in six months Jul 2001

SS7 MTP3-User Adaptation Layer (M3UA)

<draft-ietf-sigtran-m3ua-07.txt>

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as 'work in progress.'

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

To learn the current status of any Internet-Draft, please check the '1id-abstracts.txt' listing contained in the Internet- Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This Internet Draft defines a protocol for supporting the transport of any SS7 MTP3-User signalling (e.g., ISUP and SCCP messages) over IP using the services of the Stream Control Transmission Protocol. Also, provision is made for protocol elements that enable a seamless

operation of the MTP3-User peers in the SS7 and IP domains. This protocol would be used between a Signalling Gateway (SG) and a Media Gateway Controller (MGC) or IP-resident Database. It is assumed that the SG receives SS7 signalling over a standard SS7 interface using the SS7 Message Transfer Part (MTP) to provide transport.

TABLE OF CONTENTS

1. Introduction....4
1.1 Scope....4
1.2 Terminology....4
1.3 M3UA Overview....6
1.4 Functional Areas....12
1.5 Sample Configurations....21
1.6 Definition of M3UA Boundaries....24
2. Conventions....28
3. M3UA Protocol Elements....28
3.1 Common Message Header....28
3.2 Variable-Length Parameter....31
3.3 Transfer Messages....32
3.4 SS7 Signalling Network management (SSNM) Messages....35
3.5 ASP State Maintenance (ASPM) Messages....43
3.6 Routing Key Management (RKM) Messages....46
3.7 ASP Traffic Maintenance (ASPTM) Messages....55
3.8 Management(MGMT) Messages....60
4. Procedures....64
4.1 Procedures to Support the M3UA-User and Layer Management Layers....64
4.2 Procedures to Support the Management of SCTP Associations

with M3UA Peers.....67
4.3 Procedures to support the Unavailability or Congestion
Status of SS7 Destinations.....81
4.4 MTP3 Restart.....83
5. Examples of M3UA Procedures.....84
5.1 Establishment of Association and Traffic
Between SGs and ASPs.....84
5.2 ASP traffic Fail-over Examples.....89
5.3 Normal Withdrawal of an ASP from an Application Server
and Tear-down of an Association.....90
5.4.M3UA/MTP3-User Boundary Examples.....91
6. Security.....95
6.1 Introduction.....95
6.2 Threats.....95
6.3 Protecting Confidentiality.....95
7. IANA Considerations.....96
7.1 SCTP Payload Protocol Identifier.....96
7.2 M3UA Protocol Extensions.....96
8. Acknowledgements.....97
9. References.....97
10. Bibliography.....99
11. Author's Addresses.....99

1. Introduction

1.1 Scope

There is a need for Switched Circuit Network (SCN) signalling protocol delivery from an SS7 Signalling Gateway (SG) to a Media Gateway Controller (MGC) or IP-resident Database as described in the Framework Architecture for Signalling Transport [1]. The delivery mechanism SHOULD meet the following criteria:

* Support for the transfer of all SS7 MTP3-User Part messages (e.g., ISUP, SCCP, TUP, etc.)
* Support for the seamless operation of MTP3-User protocol peers
* Support for the management of SCTP transport associations and traffic between an SG and one or more MGCs or IP-resident Databases
* Support for MGC or IP-resident Database process fail-over and load-sharing
* Support for the asynchronous reporting of status changes to management

In simplistic transport terms, the SG will terminate SS7 MTP2 and MTP3 protocol layers and deliver ISUP, SCCP and/or any other MTP3-User protocol messages, as well as certain MTP network management events, over SCTP transport associations to MTP3-User peers in MGCs or IP-resident Databases.

1.2 Terminology

Application Server (AS) - A logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 SIO/DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination. The AS contains a set of one or more unique Application Server Processes, of which one or more

is normally actively processing traffic. An AS is contained within a single Network Appearance. Note that there is a 1:1 relationship between an AS and a Routing Key.

Application Server Process (ASP) - A process instance of an Application Server. An Application Server Process serves as an active or back-up process of an Application Server (e.g., part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances) of MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP end-point and may be configured to process signalling traffic within more than one Application Server.

Association - An association refers to an SCTP association. The association provides the transport for the delivery of MTP3-User protocol data units and M3UA adaptation layer peer messages.

IP Server Process (IPSP) - A process instance of an IP-based application. An IPSP is essentially the same as an ASP, except that it uses M3UA in a point-to-point fashion. Conceptually, an IPSP does not use the services of a Signalling Gateway.

Signalling Gateway Process (SGP) - A process instance of a Signalling Gateway. It serves as an active, back-up or load-sharing process of a Signalling Gateway.

Signalling Gateway - An SG is a signaling agent that receives/sends SCN

native signaling at the edge of the IP network [1]. An SG appears to the SS7 network as an SS7 Signalling Point. An SG contains a set of one or more unique Signalling Gateway Processes, of which one or more is normally actively processing traffic. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs must be coordinated into a single management view to the SS7 network and to the supported Application Servers.

Signalling Process - A process instance that uses M3UA to communicate with other signalling process. An ASP, an SGP and an IPSP are all signalling processes.

Routing Key: A Routing Key describes a set of SS7 parameters and parameter values that uniquely define the range of signalling traffic to be handled by a particular Application Server. Parameters within the Routing Key cannot extend across more than a single SS7 Destination Point Code.

Routing Context - A value that uniquely identifies a Routing Key. Routing Context values are either configured using a configuration management interface, or by using the routing key management procedures defined in this document.

Fail-over - The capability to re-route signalling traffic as required to an alternate Application Server Process, or group of ASPs, within an Application Server in the event of failure or unavailability of a currently used Application Server Process. Fail-over also applies upon the return to service of a previously unavailable Application Server Process.

Signalling Point Management Cluster (SPMC) - The complete set of Application Servers represented to the SS7 network under one specific SS7 Point Code of one specific Network Appearance. SPMCs are used to sum the availability/congestion/User_Part status of an SS7 destination point code that is distributed in the IP domain, for the

purpose of supporting MTP3 management procedures at an SG. In some

cases, the SG itself may also be a member of the SPMC. In this case, the SG availability/congestion/User_Part status must also be taken into account when considering any supporting MTP3 management actions.

MTP - The Message Transfer Part of the SS7 protocol.

MTP3 - MTP Level 3, the signalling network layer of SS7

MTP3-User - Any protocol normally using the services of the SS7 MTP3 (e.g., ISUP, SCCP, TUP, etc.).

Network Appearance û The Network Appearance uniquely identifies an SS7 entity (Point Code) into an SS7 network, as presented by the SG. It is used for the purposes of logically separating the signalling traffic between the SG and the Application Server Processes over a common SCTP association. This partitioning is necessary where an SG is logically partitioned to appear as end node elements in multiple separate SS7 networks, in which case there is a separate network appearance for each point code in the SS7 networks. It is also necessary when an SG is configured as an STP hosting multiple point codes, or when configured as multiple end nodes within the same network, in which case each point code is a separate network appearance.between the SG and the Application Server Processes over a common SCTP Association. An example is where an SG is logically partitioned to appear as an element in four separate national SS7 networks. A Network Appearance implicitly defines the SS7 Point Code(s), Network Indicator and MTP3 protocol type/variant/version used within a specific SS7 network partition.

Network Byte Order: Most significant byte first, a.k.a Big Endian.

Layer Management - Layer Management is a nodal function that handles the inputs and outputs between the M3UA layer and a local management entity.

Host - The computing platform that the ASP process is running on.

Stream - A stream refers to an SCTP stream; a uni-directional logical channel established from one SCTP endpoint to another associated SCTP endpoint, within which all user messages are delivered in-sequence except for those submitted to the un-ordered delivery service.

1.3 M3UA Overview

1.3.1 Protocol Architecture.

The framework architecture that has been defined for SCN signalling transport over IP [1] uses multiple components, including a common signalling transport protocol and an adaptation module to support the

services expected by a particular SCN signalling protocol from its underlying protocol layer.

Within the framework architecture, this document defines an MTP3-User adaptation module suitable for supporting the transfer of messages of

any protocol layer that is identified to the MTP Level 3 layer, in SS7 terms, as a user part. The list of these protocol layers include, but is not limited to, ISDN User Part (ISUP) [2,3,4], Signalling Connection Control Part (SCCP) [5,6,7] and Telephone User Part (TUP) [8]. TCAP [9,10,11] or RANAP [12] messages are transferred transparently by the M3UA protocol as SCCP payload, as they are SCCP-User protocols.

It is recommended that M3UA use the services of the Stream Control Transmission Protocol (SCTP) [13] as the underlying reliable common signalling transport protocol. This is to take advantage of various SCTP features such as:

- Explicit packet-oriented delivery (not stream-oriented),
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages,
- Optional multiplexing of user messages into SCTP datagrams,
- Network-level fault tolerance through support of multi-homing at either or both ends of an association,
- Resistance to flooding and masquerade attacks, and
- Data segmentation to conform to discovered path MTU size.

Under certain scenarios, such as back-to-back connections without redundancy requirements, the SCTP functions above MAY NOT be a requirement and TCP can be used as the underlying common transport protocol.

1.3.2 Services Provided by the M3UA Layer

The M3UA Layer at an ASP or IPSP provides the equivalent set of primitives at its upper layer to the MTP3-Users as provided by the MTP Level 3 to its local MTP3-Users at an SS7 SEP. In this way, the ISUP and/or SCCP layer at an ASP or IPSP is unaware that the expected MTP3 services are offered remotely from an MTP3 Layer at an SGP, and not by a local MTP3 layer. The MTP3 layer at an SGP may also be unaware that

its local users are actually remote user parts over M3UA. In effect, the M3UA extends access to the MTP3 layer services to a remote IP-based application. The M3UA layer does not itself provide the MTP3 services. However, in the case where an ASP is connected to more than one SGP, the
M3UA layer at an ASP must maintain the status of configured SS7 destinations and route messages according to the availability and congestion status of the routes to these destinations via each SGP.

The M3UA layer may also be used for point-to-point signalling between two IP Server Processes (IPSPs). In this case, the M3UA layer provides the same set of primitives and services at its upper layer as the MTP3. However, in this case the expected MTP3 services are not offered remotely from an SGP. The MTP3 services are provided but the procedures to support these services are a subset of the MTP3 procedures due to the simplified point-to-point nature of the IPSP to IPSP relationship.

1.3.2.1 Support for the Transport of MTP3-User Messages

The M3UA layer provides the transport of MTP-TRANSFER primitives across an established SCTP association between an SGP and an ASP or between IPSPs.

The MTP-TRANSFER primitive information is encoded as in MTP3-User messages. In this way, the SCCP and ISUP messages received from the SS7 network by the SGP are not re-encoded into a different format for

transport between the M3UA peers. The MTP3 Service Information Octet (SIO) and Routing Label (OPC, DPC, and SLS) are included, encoded as expected by the MTP3 and MTP3-User protocol layer.

At an ASP, in the case where a destination is reachable via multiple SGPs, the M3UA layer must also choose via which SGP the message is to be routed or support load balancing across the SGPs, ensuring that no missequencing occurs.

The M3UA layer does not impose a 272-octet signalling information field (SIF) length limit as specified by the SS7 MTP Level 2 protocol [14] [15] [16]. Larger information blocks can be accommodated directly by M3UA/SCTP, without the need for an upper layer segmentation/re-assembly procedure as specified in recent SCCP or ISUP versions. However, in the context of an SG, the maximum 272-octet block size must be followed when inter-working to a SS7 network that does not support the transfer of larger information blocks to the final destination. This avoids potential ISUP or SCCP fragmentation requirements at the SGPs. However, if the SS7 network is provisioned to support the Broadband MTP [20] to the final SS7 destination, the information block size limit may be increased past 272 octets.

1.3.2.2 Native Management Functions

The M3UA layer provides management of the underlying SCTP transport protocol to ensure that SGP-ASP and IPSP-IPSP transport is available to the degree called for by the MTP3-User signalling applications.

The M3UA layer provides the capability to indicate errors associated with received M3UA messages and to notify, as appropriate, local management and/or the peer M3UA.

1.3.2.3 Inter-working with MTP3 Network Management Functions

At the SGP, the M3UA layer must also provide inter-working with MTP3 management functions to support seamless operation of the user SCN signalling applications in the SS7 and IP domains. This includes:

- Providing an indication to MTP3-Users at an ASP that a remote destination in the SS7 network is not reachable.

- Providing an indication to MTP3-Users at an ASP that a remote destination in the SS7 network is now reachable.

- Providing an indication to MTP3-Users at an ASP that messages to a remote destination in the SS7 network are experiencing SS7 congestion.

- Providing an indication to the M3UA layer at an ASP that the routes to a remote destination in the SS7 network are restricted.

- Providing an indication to MTP3-Users at an ASP that a remote MTP3-User peer is unavailable.

The M3UA layer at an ASP may initiate an audit of the availability, the restricted or the congested state of remote SS7 destinations. This information is requested from the M3UA layer at the SGP.

The M3UA layer at an ASP may also indicate to the SG that the M3UA layer itself or the ASP or the ASP's Host is congested.

1.3.2.4 Support for the Management of SCTP Associations between the SGP and ASPs.

The M3UA layer at the SGP maintains the availability state of all configured remote ASPs, in order to manage the SCTP Associations and the traffic between the M3UA peers. As well, the active/inactive and congestion state of remote ASPs is maintained.

The M3UA layer MAY be instructed by local management to establish an SCTP association to a peer M3UA node. This can be achieved using the M-SCTP_ESTABLISH primitives to request, indicate and confirm the establishment of an SCTP association with a peer M3UA node. In order to avoid redundant SCTP associations between two M3UA peers, one side (client) SHOULD be designated to establish the SCTP association, or M3UA configuration knowledge maintained to detect redundant associations (e.g., via knowledge of the expected local and remote SCTP endpoint addresses).

Local management MAY request from the M3UA layer the status of the underlying SCTP associations using the M-SCTP_STATUS request and

confirm primitives. Also, the M3UA MAY autonomously inform local management of the reason for the release of an SCTP association, determined either locally within the M3UA layer or by a primitive from the SCTP.

Also the M3UA layer MAY inform the local management of the change in status of an ASP or AS. This may be achieved using the M-ASP_request or M-AS_STATUS request primitives.

1.3.2.5 Support for the Management of Connections to Multiple SGPs

As shown in Figure 1 an ASP may be connected to multiple SGPs. In such a case a particular SS7 destination may be reachable via more than one SGP, i.e., via more than one route. As MTP3 users only maintain status on a destination and not on a route basis, the M3UA layer must maintain the status (availability, restriction, and/or congestion of route to destination) of the individual routes, derive the overall availability or congestion status of the destination from the status of the individual routes, and inform the MTP3 users of this derived status whenever it changes.

1.3.3 Signalling Network Architecture

A Signalling Gateway is used to support the transport of MTP3-User signalling traffic received from the SS7 network to multiple distributed ASPs (e.g., MGCs and IP Databases). Clearly, the M3UA protocol is not designed to meet the performance and reliability requirements for such transport by itself. However, the conjunction of distributed architecture and redundant networks does allow for a sufficiently reliable transport of signalling traffic over IP. The M3UA protocol is flexible enough to allow its operation and management in a variety of physical configurations, enabling Network Operators to meet their performance and reliability requirements.

To meet the stringent SS7 signalling reliability and performance requirements for carrier grade networks, Network Operators SHOULD ensure that no single point of failure is present in the end-to-end network architecture between an SS7 node and an IP-based application. This can typically be achieved through the use of redundant SGPs or SGs, redundant hosts, and the provision of redundant QOS-bounded IP network paths for SCTP Associations between SCTP End Points. Obviously, the reliability of the SG, the MGC and other IP-based functional elements also needs to be taken into account. The distribution of ASPs and SGPs within the available Hosts SHOULD also be considered. As an example, for a particular Application Server, the related ASPs SHOULD

be distributed over at least two Hosts.

One example of a physical network architecture relevant to SS7 carrier-grade operation in the IP network domain is shown in Figure 1 below:

Sidebottom et al [Page 10]

Internet Draft SS7 MTP3-User Adaptation Layer Jul 2001

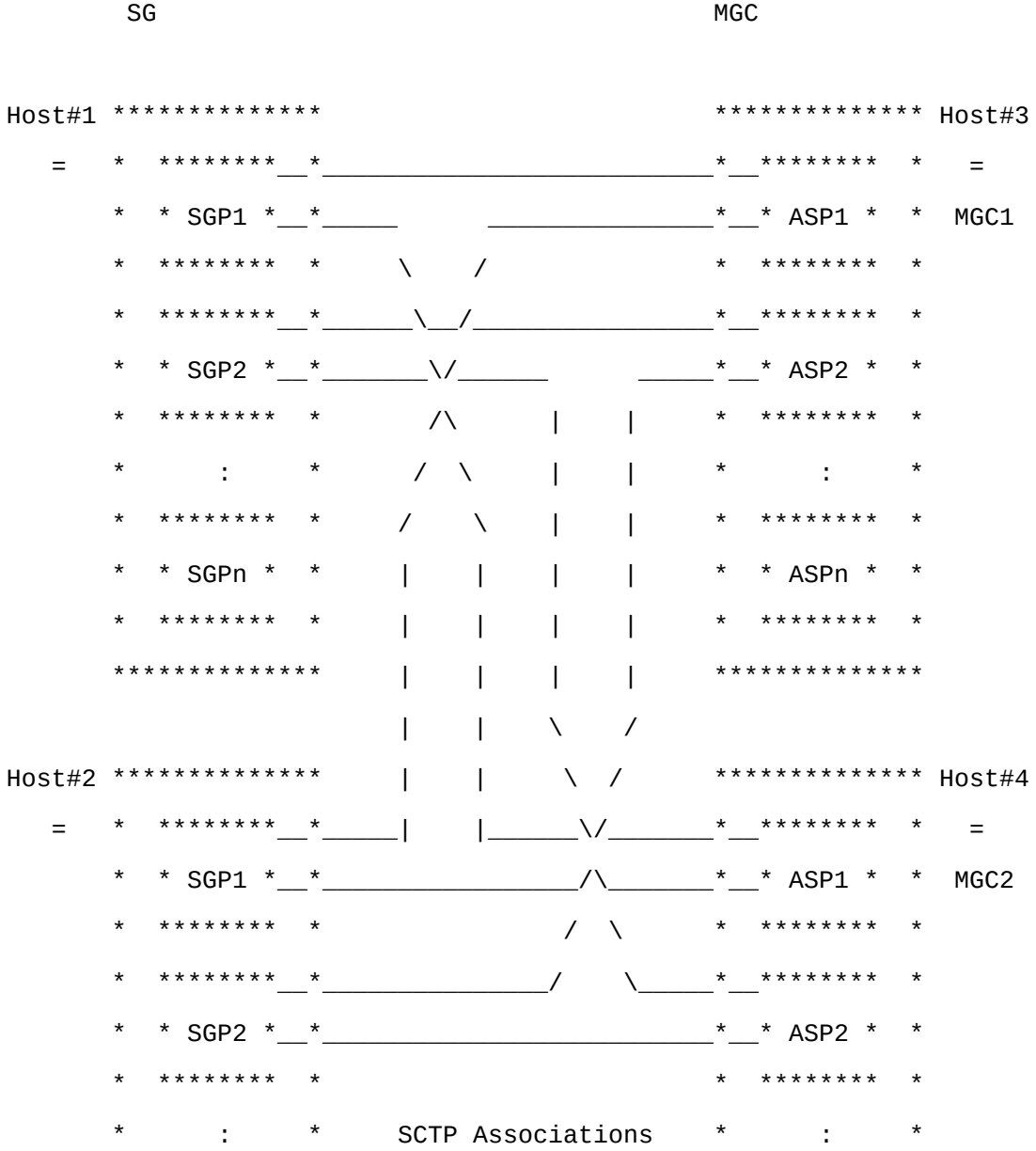




Figure 1 - Physical Model

In this model, each host has many application processes. In the case of the MGC, an ASP may provide service to one or more Application Servers, and is identified as an SCTP end point. A pair of signalling gateway processes may represent, as an example, a single Signalling Gateway, serving a signalling point management cluster.

This example model can also be applied to IPSP-IPSP signalling. In this case, each IPSP would have its services distributed across 2 hosts or more, and may have multiple server processes on each host.

In the example above, each signalling process (SGP, ASP or IPSP) is the end point to more than one SCTP association, leading to many other signalling processes. To support this, a signalling process must be able to support distribution of M3UA messages to many simultaneous active associations. This message distribution function is based on the status of provisioned routing keys, the availability of signalling points in the SS7 network, and the redundancy model (active-standby, load-sharing, n+k) of the remote signalling processes.

For carrier grade networks, the failure or isolation of a particular

signalling process SHOULD NOT cause stable calls or transactions to be lost. This implies that signalling processes need, in some cases, to share the call/transaction state or be able to pass the call state information between each other. In the case of ASPs performing call processing, coordination may also be required with the related Media Gateway to transfer the MGC control for a particular trunk termination. However, this sharing or communication of call/transaction state information is outside the scope of this document.

This model serves as an example. M3UA imposes no restrictions as to the exact layout of the network elements, the message distribution algorithms and the distribution of the signalling processes. Instead, it provides a framework and a set of messages that allow for a flexible and scalable signalling network architecture, aiming to provide reliability and performance.

1.4 Functional Areas

1.4.1 Signalling Point Code Representation

For example, within an SS7 network, a Signalling Gateway might be charged with representing a set of nodes in the IP domain into the SS7 network for routing purposes. The SG itself, as a signalling point in the SS7 network, might also be addressable with an SS7 Point Code for MTP3 Management purposes. The SG Point Code might also used for addressing any local MTP3-Users at the SG such as an SG-resident SCCP function.

An SG may be logically partitioned to operate in multiple SS7 network appearances. In such a case, the SG must be addressable with a Point Code in each network appearance, and represents a set of nodes in the IP domain into each SS7 network. Alias Point Codes [15] may also be used within an SG network appearance.

Where an SG contains more than one SGP, the MTP3 routeset, SPMC and remote AS/ASP states of each SGP SHOULD be coordinated across all the SGPs. Re-routing of traffic between the SGPs SHOULD also be supported

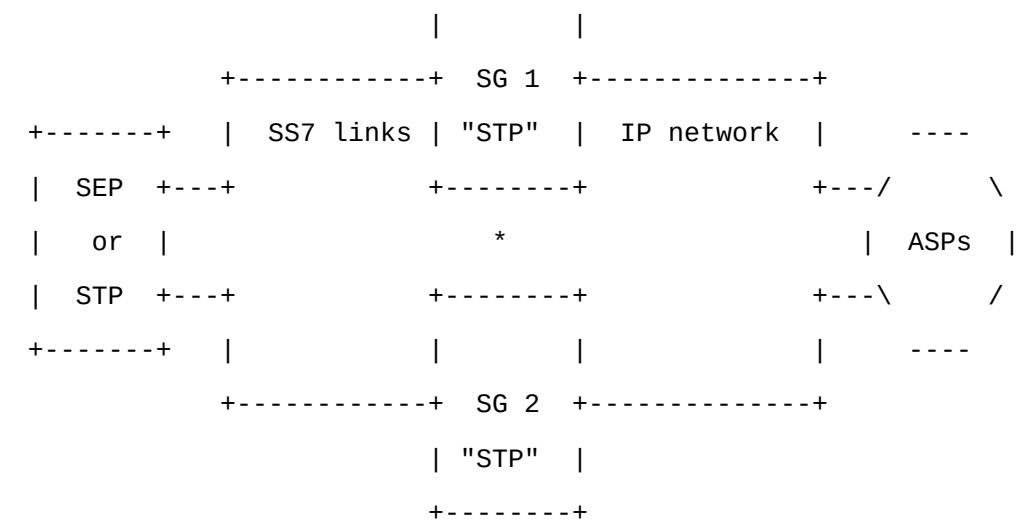
The M3UA places no restrictions on the SS7 Point Code representation of an AS. Application Servers can be represented under the same Point Code of the SG, their own individual Point Codes or grouped with other Application Servers for Point Code preservation purposes. A single Point Code may be used to represent the SG and all the Application Servers together, if desired.

If an ASP or group of ASPs is available to the SS7 network via more than one SG, each with its own Point Code, the ASP(s) should be represented by a Point Code that is separate from any SG Point Code. This allows these SGs to be viewed from the SS7 network as "STPs", each

having an ongoing "route" to the same ASP(s). Under failure conditions where the ASP(s) become(s) unavailable from one of the SGs, this approach enables MTP3 route management messaging between the SG and SS7 network, allowing simple SS7 re-routing through an alternate SG without changing the Destination Point Code Address of SS7 traffic to the ASP(s).

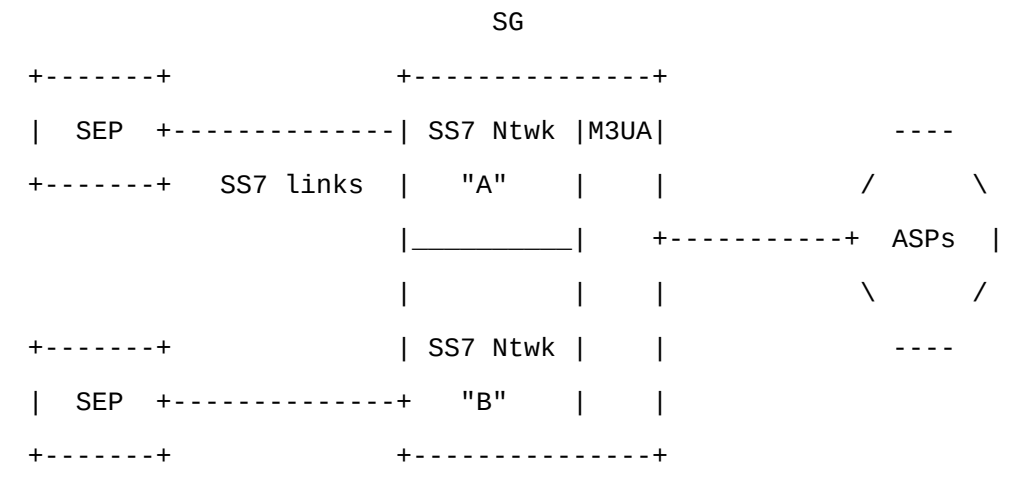
Where an AS can be reached via more than one SGP it is equally important that the corresponding Routing Keys in the involved SGPs are identical. (Note: It is possible for the SGP Routing Key configuration data to be temporarily out-of-synch during configuration updates).

+--------+



* Note:. SG-to ûSG communication is recommended for carrier grade networks, using an MTP3 linkset or an equivalent, to allow re-routing between the SGs in the event of route failures. Where SGPs are used, inter-SGP communication is recommended. Inter-SGP protocol is outside of the scope of this document.

The following example shows a signalling gateway partitioned into two network appearances.



1.4.2 Routing Contexts and Routing Keys

1.4.2.1 Overview

The distribution of SS7 messages between the SGP and the Application

Servers is determined by the Routing Keys and their associated Routing Contexts. A Routing Key is essentially a set of SS7 parameters used to

filter SS7 messages, whereas the Routing Context parameter is a 4-byte value (integer) that is associated to that Routing Key in a 1:1 relationship. The Routing Context therefore can be viewed as an index into a sending node's Message Distribution Table containing the Routing Key entries.

Possible SS7 address/routing information that comprise a Routing Key entry includes, for example, the OPC, DPC, SIO found in the MTP3 routing label, or MTP3-User specific fields such as the ISUP CIC, SCCP subsystem number, or TCAP transaction ID. Some example Routing Keys are: the DPC alone, the DPC/OPC combination, the DPC/OPC/CIC combination, or the DPC/SSN combination. The particular information used to define an M3UA Routing Key is application and network dependent, and none of the above examples are mandated.

An Application Server Process may be configured to process signalling traffic related to more than one Application Server, over a single SCTP Association. In ASP Active and ASP Inactive management messages, the signalling traffic to be started or stopped is discriminated by the Routing Context parameter. At an ASP, the Routing Context parameter uniquely identifies the range of signalling traffic associated with each Application Server that the ASP is configured to receive.

1.4.2.2 Routing Key Limitations

Routing Keys SHOULD be unique in the sense that each received SS7

signalling message SHOULD have a single routing result to an Application Server. It is not necessary for the parameter range values within a particular Routing Key to be contiguous. For example, an AS could be configured to support call processing for multiple ranges of PSTN trunks that are not represented by contiguous CIC values.

1.4.2.3 Managing Routing Contexts and Routing Keys

There are two ways to provision a Routing Key at an SGP. A Routing Key may be configured statically using an implementation dependent management interface, or dynamically using the M3UA Routing Key registration procedure. A Routing Key may also be configured using the M3UA dynamic registration/deregistration procedures defined in this document. An M3UA element must implement at least one method of Routing Key provisioning.

When using a management interface to configure Routing Keys, the message distribution function within the SGP is not limited to the set of parameters defined in this document. Other implementation dependent distribution algorithms may be used.

1.4.2.4 Message Distribution at the SGP

In order to direct messages received from the SS7 MTP3 network to the

appropriate IP destination, the SGP must perform a message distribution function using information from the received MTP3-User message.

To support this message distribution, the SGP must maintain the equivalent of a network address translation table, mapping incoming SS7 message information to an Application Server for a particular application and range of traffic. This is accomplished by comparing elements of the incoming SS7 message to currently defined Routing Keys in the SGP. These Routing Keys in turn make reference to an Application Server that is enabled by one or more ASPs. These ASPs provide dynamic status information on their availability, traffic handling capability and congestion to the SGP using various management messages defined in the M3UA protocol.

The list of ASPs in an AS is assumed to be dynamic, taking into account the availability, traffic handling capability and congestion status of the individual ASPs in the list, as well as configuration changes and possible fail-over mechanisms.

Normally, one or more ASPs are active in the AS (i.e., currently processing traffic) but in certain failure and transition cases it is possible that there may be no active ASP available. Both load-sharing and backup scenarios are supported.

When there is no matching Routing Key entry for an incoming SS7 message, a default treatment SHOULD be specified. Possible solutions are to provide a default Application Server at the SGP that directs all unallocated traffic to a (set of) default ASP(s), or to drop the message and provide a notification to layer management. The treatment of unallocated traffic is implementation dependent.

1.4.2.5 Message Distribution at the ASP

In order to direct messages to the SS7 network, the ASP must also perform a message distribution function in order to choose the proper

SGP for a given message. This is accomplished by observing the Destination Point Code (and possibly other elements of the outgoing message such as the SLS value).Where more than one route (or SGP) is possible for routing to the SS7 network, the ASP SHOULD maintain a dynamic table of available SGP routes for the SS7 destinations, taking into account the SS7 destination availability/restricted/congestion status received from the SGP(s), the availability status of the individual SGPs and configuration changes and fail-over mechanisms. There is, however, no M3UA messaging to manage the status of an SGP (e.g., SGP-Up/Down/Active/Inactive messaging). Whenever an SCTP

association to an SGP exists, the SGP is assumed to be ready for the purposes of responding to M3UA ASPSM messages.

Every SGP of one SG ASP regarding one AS provides identical SS7 connectivity to this ASP.

1.4.3 SS7 and M3UA Interworking

In the case of SS7 and M3UA inter-working, the M3UA adaptation layer is designed to provide an extension of the MTP3 defined user primitives.

1.4.3.1 Signalling Gateway SS7 Layers

The SG is responsible for terminating MTP Level 3 of the SS7 protocol, and offering an IP-based extension to its users.

>From an SS7 perspective, it is expected that the Signalling Gateway transmits and receives SS7 Message Signalling Units (MSUs) to and

from the PSTN over a standard SS7 network interface, using the SS7 Message Transfer Part (MTP) [14,15,16] to provide reliable transport of the messages.

As a standard SS7 network interface, the use of MTP Level 2 signalling links is not the only possibility. ATM-based High Speed Links can also be used with the services of the Signalling ATM Adaptation Layer (SAAL) [17,18].

Note: It is also possible for IP-based interfaces to be present, using the services of the MTP2-User Adaptation Layer (M2UA) [23] or M2PA []. These may be terminated at a Signalling Transfer Point (STP) or Signalling End Point (SEP). Using the services of MTP3, the SG may be capable of communicating with remote SS7 SEPs in a quasi-associated fashion, where STPs may be present in the SS7 path between the SEP and the SG.

1.4.3.2 SS7 and M3UA Inter-Working at the SG

The SGP provides a functional inter-working of transport functions between the SS7 network and the IP network by also supporting the M3UA adaptation layer. It allows the transfer of MTP3-User signalling messages to and from an IP-based Application Server Process where the peer MTP3-User protocol layer exists.

The Signalling Gateway must maintain knowledge of relevant SS7 node and Signalling Point Management Cluster (SPMC) status in their respective domains in order to perform a seamless inter-working of the IP-based signalling and the SS7 domains. For example, SG knowledge of the availability and/or congestion status of the SPMC and SS7 nodes must be maintained and disseminated in the respective networks, in order to ensure that end-to-end operation is transparent to the communicating SCN protocol peers at the SS7 node and ASP. Where more than one SGP

constitutes an SG, the knowledge of the SGPs must be coordinated into an overall SG view.

For SS7 user part management, it is required that the MTP3-User protocols at ASPs receive indications of SS7 signalling point availability, SS7 network congestion, and remote User Part unavailability as would be expected in an SS7 SEP node. To accomplish this, the MTP-PAUSE, MTP-RESUME and MTP-STATUS indication primitives received at the MTP3 upper layer interface at the SG need to be propagated to the remote MTP3-User lower layer interface at the ASP. (These indication primitives are also made available to any existing local MTP3-Users at the SG, if present.)

MTP3 management messages (such as TFPs or TFAs received from the SS7 network) MUST NOT be encapsulated as Data message Payload Data and sent either from SG to ASP or from ASP to SG. The SG MUST terminate these messages and generate M3UA messages as appropriate.

1.4.3.3 Application Server

A cluster of application servers is responsible for providing the overall support for one or more SS7 upper layers. From an SS7 standpoint, a Signalling Point Management Cluster (SPMC) provides complete support for the upper layer service for a given point code. As an example, an SPMC providing MGC capabilities must provide complete support for ISUP (and any other MTP3 user located at the point code of the SPMC) for a given point code, according to the local SS7 network specifications.

This measure is necessary to allow the SG to accurately represent the signalling point on the local SS7 network.

In the case where an ASP is connected to more than one SGP, the M3UA layer must maintain the status of configured SS7 destinations and route messages according to availability/congestion/restricted status of the routes to these SS7 destinations.

1.4.3.4 IPSP Considerations

Since IPSPs use M3UA in a point-to-point fashion, there is no concept of routing of messages beyond the remote end. Therefore, SS7 and M3UA inter-working is not necessary for this model.

1.4.4 Redundancy Models

The network address translation and mapping function of the M3UA layer supports signalling process fail-over functions in order to support a high availability of call and transaction processing capability.

1.4.4.1 Application Server Redundancy

All MTP3-User messages (e.g., ISUP, SCCP) incoming to an SG from the SS7 network are assigned to a unique Application Server, based on the information in the message and the provisioned Routing Keys.

The Application Server is, in practical terms, a list of all ASPs configured to process a range of MTP3-User traffic defined by one Routing Key. One or more ASPs in the list are normally active (i.e.,

handling traffic) while any others may be unavailable or inactive, to be possibly used in the event of failure or unavailability of the active ASP(s).

The fail-over model supports an "n+k" redundancy model, where "n" ASPs is the minimum number of redundant ASPs required to handle traffic and "k" ASPs are available to take over for a failed or unavailable ASP. A "1+1" active/back-up redundancy is a subset of this model. A simplex "1+0" model is also supported as a subset, with no ASP redundancy.

At the SGP, an Application Server list contains active and inactive ASPs to support ASP load-sharing and fail-over procedures. The list of ASPs within a logical Application Server is kept updated in the SGP to reflect the active Application Server Process(es).

To avoid a single point of failure, it is recommended that a minimum of two ASPs be in the list, resident in separate hosts and therefore available over different SCTP Associations. For example, in the network shown in Figure 1, all messages to DPC x could be sent to ASP1 in Host3 or ASP1 in Host4. The AS list at SGP1 in Host 1 might look like the following:

```
    Routing Key {DPC=x) - "Application Server #1"
        ASP1/Host3  - State = Active
        ASP1/Host3  - State = Inactive
```

In this "1+1" redundancy case, ASP1 in Host3 would be sent any incoming message with DPC=x. ASP1 in Host4 would normally be brought to the "active" state upon failure of, or loss of connectivity to, ASP1/Host1.

The AS List at SGP1 in Host1 might also be set up in load-share mode:

```
    Routing Key {DPC=x) - "Application Server #1"
        ASP1/Host3 - State = Active
        ASP1/Host4 - State = Active
```

In this case, both the ASPs would be sent a portion of the traffic. For example the two ASPs could together form a database, where incoming queries may be sent to any active ASP.

Care must be exercised by a Network Operator in the selection of the routing information to be used as the Routing Key for a particular AS.

For example, where Application Servers are defined using ranges of ISUP CIC values, the Operator is implicitly splitting up control of the related circuit groups. Some CIC value range assignments may interfere with ISUP circuit group management procedures.

In the process of fail-over, it is recommended that in the case of ASPs supporting call processing, stable calls do not fail. It is possible that calls in "transition" MAY fail, although measures of communication between the ASPs involved can be used to mitigate this. For example, the two ASPs MAY share call state via shared memory, or MAY use an ASP to ASP protocol to pass call state information. Any ASP-to-ASP protocol to support this function is outside the scope of this document.

1.4.4.2 Signalling Gateway Redundancy

Signalling Gateways MAY also be distributed over multiple hosts. Much like the AS model, SGs may comprise one or more SG Processes (SGPs), distributed over one or more hosts, using an active/back-up or a load-sharing model. Also, every SGP within an SG communicating with an ASP provides identical SS7 connectivity to this ASP. Should an SGP lose all or partial SS7 connectivity and other SGPs exist, the SGP SHOULD

terminate the SCTP associations to the concerned ASPs.

It is therefore possible for an ASP to route signalling messages destined to the SS7 network using more than one SGP. In this model, a Signalling Gateway is deployed as a cluster of hosts acting as a single SG. A primary/back-up redundancy model is possible, where the unavailability of the SCTP association to a primary SGP could be used to reroute affected traffic to an alternate SGP. A load-sharing model is possible, where the signalling messages are load-shared between multiple SGPs. The distribution of the MTP3-user messages over the SGPs should be done in such a way to minimize message mis-sequencing, as required by the SS7 User Parts.

It may also be possible for an ASP to use more than one SG to access a specific SS7 end point, in a model that resembles an SS7 STP mated pair. Typically, SS7 STPs are deployed in mated pairs, with traffic load-shared between them. Other models are also possible, subject to the limitations of the local SS7 network provisioning guidelines.

>From the perspective of the M3UA layer at an ASP, a particular SG is capable of transferring traffic to an SS7 destination if an SCTP association with at least one SGP of the SG is established, the SGP has returned an acknowledgement to the ASP to indicate that the ASP is actively handling traffic for that destination, and the SGP has not indicated that the destination is inaccessible. When an ASP is configured to use multiple SGPs for transferring traffic to the SS7 network, the ASP must maintain knowledge of the current capability of the SGPs to handle traffic to destinations of interest. This information is crucial to the overall reliability of the service, for

both active/back-up and load-sharing model, in the event of failures, recovery and maintenance activities. The ASP M3UA may also use this information for congestion avoidance purposes. The distribution of the MTP3-user messages over the SGPs should be done in such a way to minimize message mis-sequencing, as required by the SS7 User Parts.

1.4.5 Flow Control

Local Management at an ASP may wish to stop traffic across an SCTP association in order to temporarily remove the association from service or to perform testing and maintenance activity. The function could optionally be used to control the start of traffic on to a newly available SCTP association.

1.4.6 Congestion Management

The M3UA layer is informed of local and IP network congestion by means of an implementation-dependent function (e.g., an implementation-dependent indication from the SCTP of IP network congestion).

At an ASP or IPSP, the M3UA layer indicates congestion to local MTP3-Users by means of an MTP-STATUS primitive, as per current MTP3 procedures, to invoke appropriate upper layer responses.

When an SG determines that the transport of SS7 messages to a Signalling Point Management Cluster (SPMC) is encountering congestion, the SG MAY trigger SS7 MTP3 Transfer Controlled management messages to originating SS7 nodes, per the congestion procedures of the relevant MTP3 standard. The triggering of SS7 MTP3 Management messages from an SG is an implementation-dependent function.

The M3UA layer at an ASP or IPSP should indicate local congestion to an M3UA peer with an SCON message. When an SG receives a congestion message (SCON) from an ASP, and the SG determines that an SPMC is now encountering congestion, it MAY trigger SS7 MTP3 Transfer Controlled management messages to concerned SS7 destinations according to

congestion procedures of the relevant MTP3 standard.

1.4.7 SCTP Stream Mapping.

The M3UA layer at both the SGP and ASP also supports the assignment of signalling traffic into streams within an SCTP association. Traffic that requires sequencing must be assigned to the same stream. To accomplish this, MTP3-User traffic may be assigned to individual streams based on, for example, the SLS value in the MTP3 Routing Label or the ISUP CIC assignment, subject of course to the maximum number of streams supported by the underlying SCTP association.

The use of SCTP streams within M3UA is recommended in order to minimize transmission and buffering delays, therefore improving the overall performance and reliability of the signalling elements. The distribution of the MTP3 user messages over the various streams should

be done in such a way to minimize message mis-sequencing, as required by the SS7 User Parts.

1.4.8 Client/Server Model

It is recommended that the SGP and ASP be able to support both client and server operation. The peer endpoints using M3UA SHOULD be configured so that one always takes on the role of client and the other the role of server for initiating SCTP associations. The default orientation would be for the SGP to take on the role of server while the ASP is the client. In this case, ASPs SHOULD initiate the SCTP association to the SGP

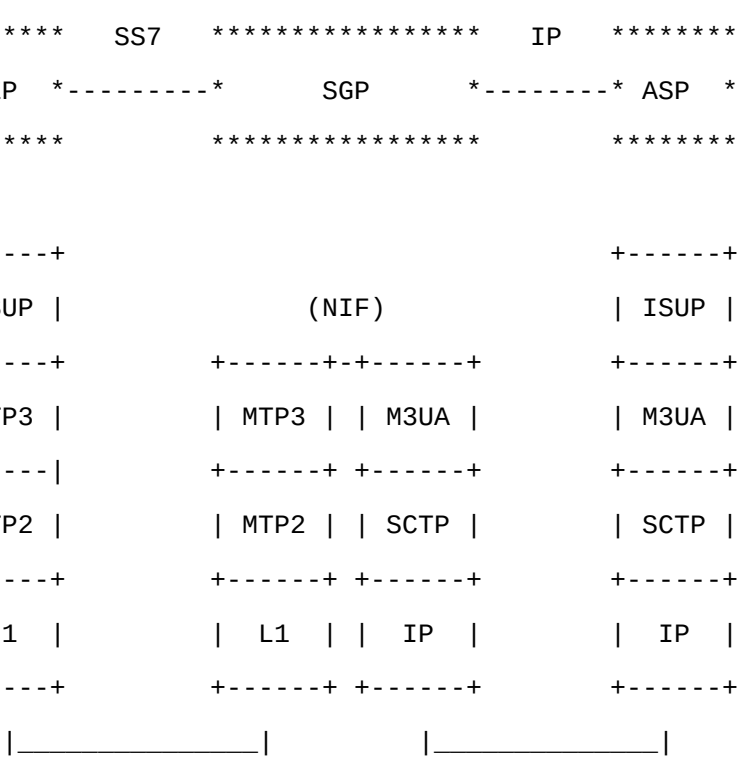
In the case of IPSP to IPSP communication, the peer endpoints using

M3UA SHOULD be configured so that one always takes on the role of client and the other the role of server for initiating SCTP associations.

The SCTP Registered User Port Number Assignment for M3UA is 2905.

1.5 Sample Configurations

1.5.1 Example 1: ISUP Message Transport



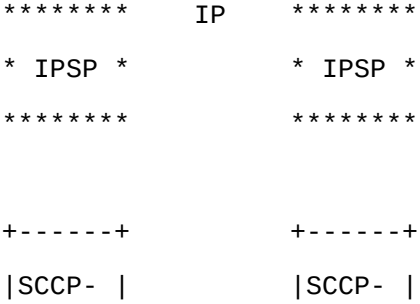
SEP - SS7 Signalling End Point
SCTP - Stream Control Transmission Protocol
NIF - Nodal Inter-working Function

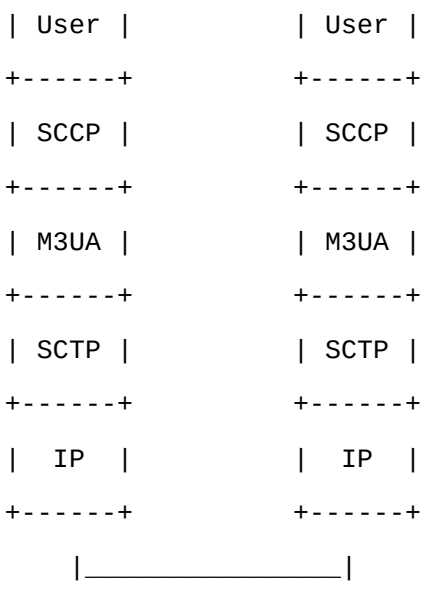
In this example, the SGP provides an implementation-dependent nodal inter-working function (NIF) that allows the MGC to exchange SS7 signalling messages with the SS7-based SEP. The NIF within the SGP serves as the interface within the SGP between the MTP3 and M3UA. This nodal inter-working function has no visible peer protocol with either

the MGC or SEP. It also provides network status information to one or both sides of the network.

For internal SGP modeling purposes, at the NIF level, SS7 signalling messages that are destined to the MGC are received as MTP-TRANSFER indication primitives from the MTP Level 3 upper layer interface, translated to MTP-TRANSFER request primitives, and sent to the local M3UA-resident message distribution function for ongoing routing to the final IP destination. Messages received from the local M3UA network address translation and mapping function as MTP-TRANSFER indication primitives are sent to the MTP Level 3 upper layer interface as MTP-TRANSFER request primitives for on-going MTP Level 3 routing to an SS7 SEP. For the purposes of providing SS7 network status information the NIF also delivers MTP-PAUSE, MTP-RESUME and MTP-STATUS indication primitives received from the MTP Level 3 upper layer interface to the local M3UA-resident management function. In addition, as an implementation and network option, restricted destinations are communicated from MTP network management to the local M3UA-resident management function.

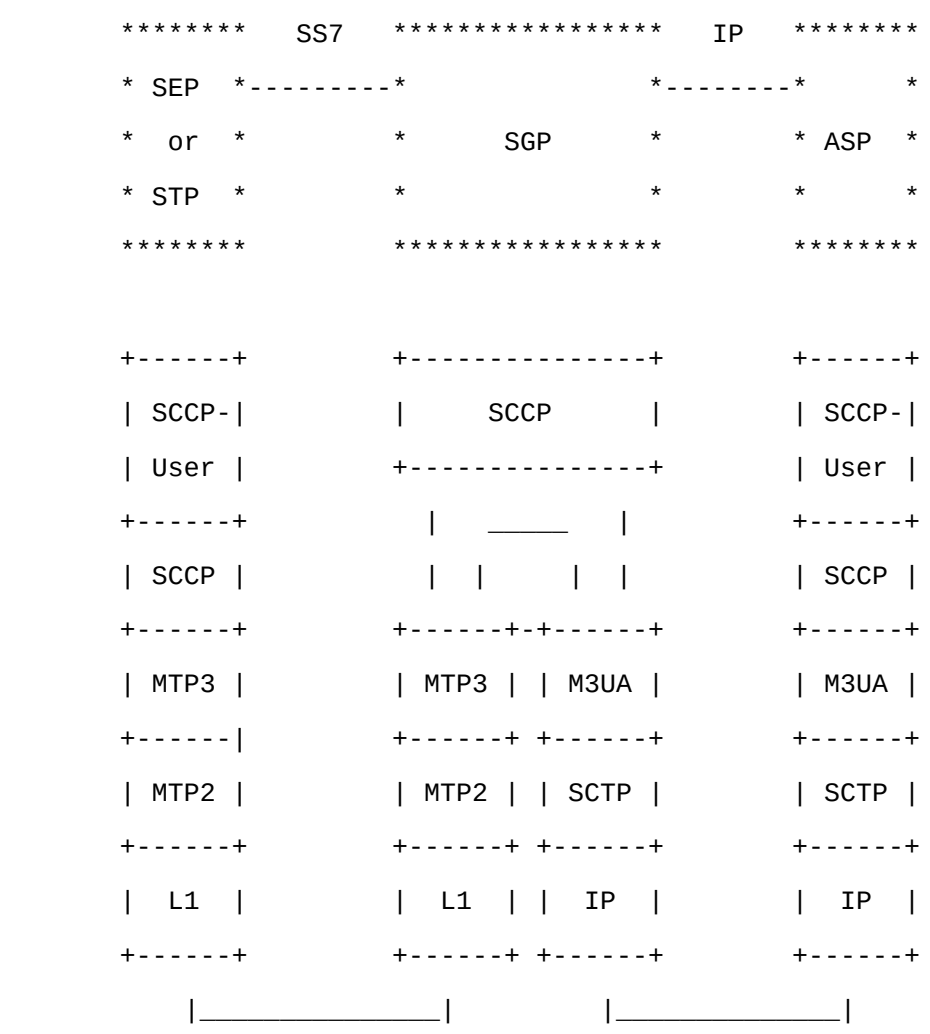
1.5.2 Example 2: SCCP Transport between IPSPs





This example shows an architecture where no Signalling Gateway is used. In this example, SCCP messages are exchanged directly between two IP-resident IPSPs with resident SCCP-User protocol instances, such as RANAP or TCAP. SS7 network inter-working is not required, therefore there is no MTP3 network management status information for the SCCP and SCCP-User protocols to consider. Any MTP-PAUSE, MTP-RESUME or MTP-STATUS indications from the M3UA layer to the SCCP layer should consider the status of the SCTP Association and underlying IP network and any congestion information received from the remote site.

1.5.3 Example 3: SGP Resident SCCP Layer, with Remote ASP



STP - SS7 Signalling Transfer Point

In this example, the SGP contains an instance of the SS7 SCCP protocol layer that may, for example, perform the SCCP Global Title Translation (GTT) function for messages logically addressed to the SG SCCP. If the result of a GTT for an SCCP message yields an SS7 DPC or DPC/SSN address of an SCCP peer located in the IP domain, the resulting MTP-TRANSFER request primitive is sent to the local M3UA-resident network address translation and mapping function for ongoing routing to the final IP destination.

Similarly, the SCCP instance in an SGP can perform the SCCP GTT service for messages logically addressed to it from SCCP peers in the IP domain. In this case, MTP-TRANSFER indication primitives are sent from the local M3UA-resident network address translation and mapping

function to the SCCP for GTT. If the result of the GTT yields the address of an SCCP peer in the SS7 network then the resulting MTP-TRANSFER request primitive is given to the MTP3 for delivery to an SS7-resident node.

It is possible that the above SCCP GTT at the SGP could yield the address of an SCCP peer in the IP domain and the resulting MTP-TRANSFER request primitive would be sent back to the M3UA layer for delivery to an IP destination.

For internal SGP modeling purposes, this may be accomplished with the use of an implementation-dependent nodal inter-working function within the SGP that effectively sits below the SCCP and routes MTP-TRANSFER

request/indication messages to/from both the MTP3 and the M3UA layer, based on the SS7 DPC or DPC/SSN address information. This nodal inter-working function has no visible peer protocol with either the ASP or SEP.

Note that the services and interface provided by the M3UA layer are the same as in Example 1 and the functions taking place in the SCCP entity are transparent to the M3UA layer. The SCCP protocol functions are not reproduced in the M3UA protocol.

1.6 Definition of M3UA Boundaries

1.6.1 Definition of the Boundary between M3UA and an MTP3-User.

>From ITU Q.701 [14]:

MTP-TRANSFER request

MTP-TRANSFER indication

MTP-PAUSE indication

MTP-RESUME indication

MTP-STATUS indication

1.6.2 Definition of the Boundary between M3UA and SCTP

An example of the upper layer primitives provided by the SCTP are provided in Reference [13] Section 10.

1.6.3 Definition of the Boundary between M3UA and Layer Management

M-SCTP_ESTABLISH request

Direction: LM -> M3UA

Purpose: LM requests ASP to establish an SCTP association with its peer.

M-STCP_ESTABLISH confirm

Direction: M3UA -> LM

Purpose: ASP confirms to LM that it has established an SCTP association with its peer.

M-SCTP_ESTABLISH indication

Direction: M3UA -> LM

Purpose: M3UA informs LM that a remote ASP has established an SCTP association.

M-SCTP_RELEASE request

Direction: LM -> M3UA

Purpose: LM requests ASP to release an SCTP association with its peer.

M-SCTP_RELEASE confirm

Direction: M3UA -> LM

Purpose: ASP confirms to LM that it has released SCTP association with its peer.

M-SCTP_RELEASE indication

Direction: M3UA -> LM

Purpose: M3UA informs LM that a remote ASP has released an SCTP Association or the SCTP association has failed.

M-SCTP_STATUS request

Direction: LM -> M3UA

Purpose: LM requests M3UA to report the status of an SCTP association.

M-SCTP_STATUS confirm

Direction: M3UA -> LM

Purpose: M3UA responds with the status of an SCTP association.

M-SCTP STATUS indication

Direction: M3UA -> LM

Purpose: M3UA reports the status of an SCTP association.

M-ASP_STATUS request

Direction: LM -> M3UA

Purpose: LM requests M3UA to report the status of a local or remote ASP.

M-ASP_STATUS confirm

Direction: M3UA -> LM

Purpose: M3UA reports status of local or remote ASP.

M-AS_STATUS request

Direction: LM -> M3UA

Purpose: LM requests M3UA to report the status of an AS.

M-AS_STATUS confirm

Direction: M3UA -> LM

Purpose: M3UA reports the status of an AS.

M-NOTIFY indication

Direction: M3UA -> LM

Purpose: M3UA reports that it has received a Notify message
from its peer.

M-ERROR indication

Direction: M3UA -> LM

Purpose: M3UA reports that it has received an Error message from
its peer or that a local operation has been unsuccessful.

M-ASP_UP request

Direction: LM -> M3UA

Purpose: LM requests ASP to start its operation and send an ASP Up
message to its peer.

M-ASP_UP confirm

Direction: M3UA -> LM

Purpose: ASP reports that is has received an ASP UP Ack message from

its peer.

M-ASP_UP indication

Direction: M3UA -> LM

Purpose: M3UA reports it has successfully processed an incoming ASP Up message from its peer.

M-ASP_DOWN request

Direction: LM -> M3UA

Purpose: LM requests ASP to stop its operation and send an ASP-Down message to its peer.

M-ASP_DOWN confirm

Direction: M3UA -> LM

Purpose: ASP reports that is has received an ASP Down Ack message from its peer.

M-ASP_DOWN indication

Direction: M3UA -> LM

Purpose: M3UA reports it has successfully processed an incoming ASP Down message from its peer, or the SCTP association has been lost/reset.

M-ASP_ACTIVE request

Direction: LM -> M3UA

Purpose: LM requests ASP to send an ASP Active message to its peer.

M-ASP_ACTIVE confirm

Direction: M3UA -> LM

Purpose: ASP reports that is has received an ASP Active Ack message from its peer.

M-ASP_ACTIVE indication

Direction: M3UA -> LM

Purpose: M3UA reports it has successfully processed an incoming ASP

Active message from its peer.

M-ASP_INACTIVE request
Direction: LM -> M3UA
Purpose: LM requests ASP to send an ASP Inactive message to its peer.

M-ASP_INACTIVE confirm
Direction: LM -> M3UA
Purpose: ASP reports that is has received an ASP Inactive Ack message from its peer.

M-ASP_INACTIVE indication
Direction: M3UA -> LM
Purpose: M3UA reports it has successfully processed an incoming ASP Inactive message from its peer.

M-AS_ACTIVE indication
Direction: M3UA -> LM
Purpose: M3UA reports that an AS has moved to the AS-ACTIVE state.

M-AS_INACTIVE indication
Direction: M3UA -> LM
Purpose: M3UA reports that an AS has moved to the AS-INACTIVE state.

M-AS_DOWN indication
Direction: M3UA -> LM

Purpose: M3UA reports that an AS has moved to the AS-DOWN state.

If dynamic registration of RK is supported by the M3UA layer, the layer MAY support the following additional primitives:

M-RK_REG request
Direction: LM -> M3UA
Purpose: LM requests ASP to register RK(s) with its peer by sending REG REQ message

M-RK_REG confirm
Direction: M3UA -> LM
Purpose: ASP reports that it has received REG RSP message with registration status as successful from its peer.

M-RK_REG indication
Direction: M3UA -> LM
Purpose: M3UA informs LM that it has successfully processed an incoming REG REQ message.

M-RK_DEREG request
Direction: LM -> M3UA
Purpose: LM requests ASP to de-register RK(s) with its peer by sending DEREG REQ message.

M-RK_DEREG confirm
Direction: M3UA -> LM
Purpose: ASP reports that it has received DEREG REQ message with de-registration status as successful from its peer.

M-RK_DEREG indication

Direction: M3UA -> LM

Purpose: M3UA informs LM that it has successfully processed an incoming DEREG REQ from its peer.

2.0 Conventions

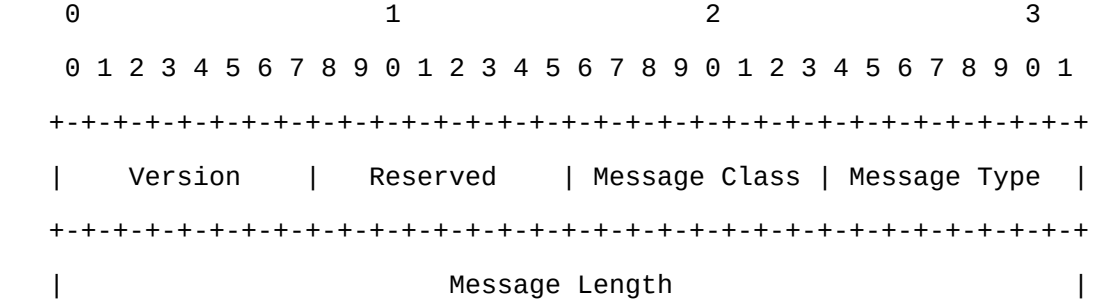
The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

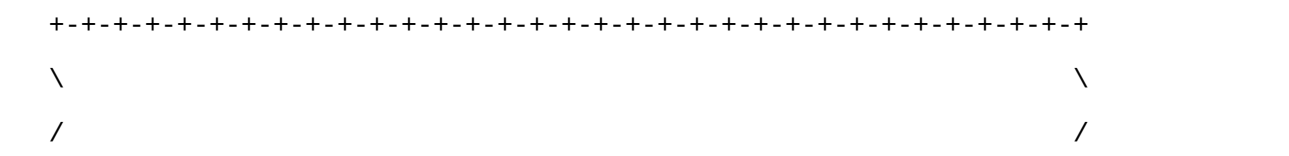
3. M3UA Protocol Elements

The general M3UA message format includes a Common Message Header followed by zero or more parameters as defined by the Message Type. For forward compatibility, all Message Types may have attached parameters even if none are specified in this version.

3.1 Common Message Header

The protocol messages for MTP3-User Adaptation require a message header which contains the adaptation layer version, the message type, and message length.





All fields in an M3UA message MUST be transmitted in the network byte order, unless otherwise stated.

3.1.1 M3UA Protocol Version: 8 bits (unsigned integer)

The version field contains the version of the M3UA adaptation layer.

The supported versions are the following:

1 Release 1.0

3.1.2 Message Classes and Types

The following list contains the valid Message Classes:

Message Class: 8 bits (unsigned integer)

The following list contains the valid Message Type Classes:

0 Management (MGMT) Message
1 Transfer Messages
2 SS7 Signalling Network Management (SSNM) Messages

```
     3     ASP State Maintenance (ASPSM) Messages
     4     ASP Traffic Maintenance (ASPTM) Messages
     5     Reserved for Other Sigtran Adaptation Layers
     6      Reserved for Other Sigtran Adaptation Layers
     7     Reserved for Other Sigtran Adaptation Layers
     8     Reserved for Other Sigtran Adaptation Layers
     9     Routing Key Management (RKM) Messages
  10 to 127 Reserved by the IETF
 128 to 255 Reserved for IETF-Defined Message Class extensions

Message Type: 8 bits (unsigned integer)

   The following list contains the message types for the defined
   messages.

     Management (MGMT) Messages (See Section 3.6)

         0        Error (ERR)
         1        Notify (NTFY)
      2 to 127    Reserved by the IETF
    128 to 255    Reserved for IETF-Defined MGMT extensions

     Transfer Messages (See Section 3.3)

         0        Reserved
         1        Payload Data (DATA)
      2 to 127    Reserved by the IETF
    128 to 255    Reserved for IETF-Defined Transfer extensions

     SS7 Signalling Network Management (SSNM) Messages (See Section
3.4)

         0        Reserved
         1        Destination Unavailable (DUNA)
         2        Destination Available (DAVA)
```

```
         3        Destination State Audit (DAUD)
         4        SS7 Network Congestion (SCON)
         5        Destination User Part Unavailable (DUPU)
         6        Destination Restricted (DRST)
      7 to 127    Reserved by the IETF
    128 to 255    Reserved for IETF-Defined SSNM extensions
```



```
  ASP State Maintenance (ASPSM) Messages (See Section 3.5)

         0        Reserved
         1        ASP Up (ASPUP)
         2        ASP Down (ASPDN)
         3        Heartbeat (BEAT)
         4        ASP Up Acknowledgement (ASPUP ACK)
         5        ASP Down Acknowledgement (ASPDN ACK)
         6        Heatbeat Acknowledgement (BEAT ACK)
      7 to 127    Reserved by the IETF
    128 to 255    Reserved for IETF-Defined ASPSM extensions

  ASP Traffic Maintenance (ASPTM) Messages (See Section 3.5)

         0        Reserved
         1        ASP Active (ASPAC)
         2        ASP Inactive (ASPIA)
         3        ASP Active Acknowledgement (ASPAC ACK)
         4        ASP Inactive Acknowledgement (ASPIA ACK)
      5 to 127    Reserved by the IETF
    128 to 255    Reserved for IETF-Defined ASPTM extensions

  Routing Key Management (RKM) Messages (See Section 3.7)
```

0	Reserved
1	Registration Request (REG REQ)
2	Registration Response (REG RSP)
3	Deregistration Request (DEREG REQ)
4	Deregistration Response (DEREG RSP)
5 to 127	Reserved by the IETF
128 to 255	Reserved for IETF-Defined RKM extensions

3.1.3 Reserved: 8 bits

The Reserved field SHOULD be set to all '0's and ignored by the receiver.

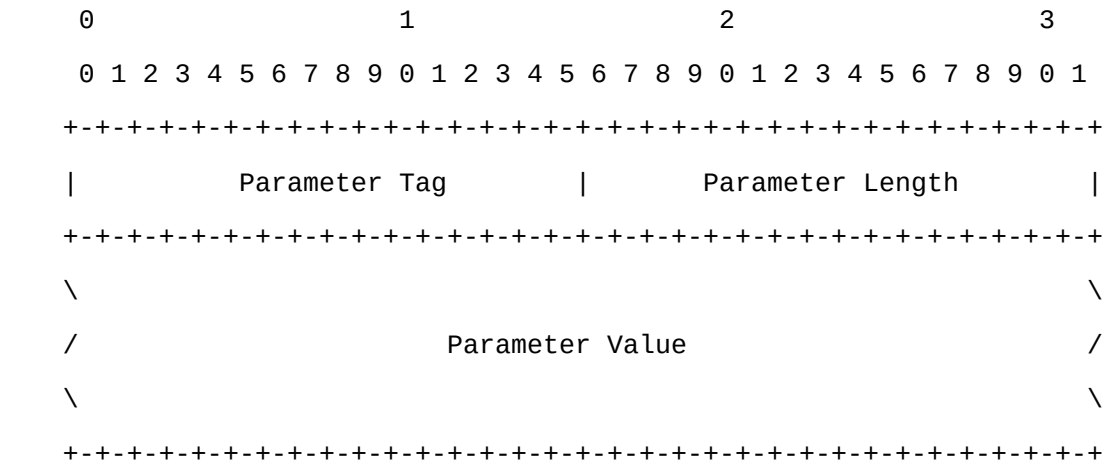
3.1.4 Message Length: 32-bits (unsigned integer)

The Message Length defines the length of the message in octets, including the Common Header. For messages with a final parameter containing padding, the parameter padding MUST be included in the Message Length.

Note: A receiver SHOULD accept the message whether or not the final parameter padding is included in the message length.

3.2 Variable-Length Parameter Format

M3UA messages consist of a Common Header followed by zero or more variable length parameters, as defined by the message type. All the parameters contained in a message are defined in a Tag-Length-Value format as shown below.



Where more than one parameter is included in a message, the parameters may be in any order, except where explicitly mandated. A receiver SHOULD accept the parameters in any order.

Parameter Tag: 16 bits (unsigned integer)

The Tag field is a 16-bit identifier of the type of parameter. It takes a value of 0 to 65534. Common parameters used by adaptation layers are in the range of 0x00 to 0xff. M3UA-specific parameters have Tags in the range 0x80 to 0xbf. The parameter Tags defined are as follows:

0x00	Reserved
0x80	Network Appearance
0x81	Protocol Data 1
0x82	Protocol Data 2
0x04	INFO String
0x83	Affected Destinations
0x06	Routing Context
0x07	Diagnostic Information

```
         0x09        Heartbeat Data
         0x84        User/Cause
         0x0a        Reason
         0x0b        Traffic Mode Type
         0x0c        Error Code
         0x0d        Status
         0x85        Congestion Indications
         0x86        Concerned Destination
         0x87        Routing Key
         0x88        Registration Result
         0x89        De-registration Result
         0x8a        Local_Routing Key Identifier
         0x8b        Destination Point Code
         0x8c        Service Indicators
```



```
         0x8d        Subsystem Numbers
         0x8e        Originating Point Code List
         0x8f        Circuit Range
         0x90        Registration Results
         0x91        De-Registration Results
      0x92 to ffff...Reserved by the IETF
```

The value of 65535 is reserved for IETF-defined extensions. Values other than those defined in specific parameter description are reserved for use by the IETF.

Parameter Length: 16 bits (unsigned integer)

The Parameter Length field contains the size of the parameter in

bytes, including the Parameter Tag, Parameter Length, and Parameter Value fields. The Parameter Length does not include any padding bytes.

Parameter Value: variable-length.

The Parameter Value field contains the actual information to be transferred in the parameter.

The total length of a parameter (including Tag, Parameter Length and Value fields) MUST be a multiple of 4 bytes. If the length of the parameter is not a multiple of 4 bytes, the sender pads the Parameter at the end (i.e., after the Parameter Value field) with all zero bytes. The length of the padding is NOT included in the parameter length field. A sender SHOULD NOT pad with more than 3 bytes. The receiver MUST ignore the padding bytes.

3.3 Transfer Messages

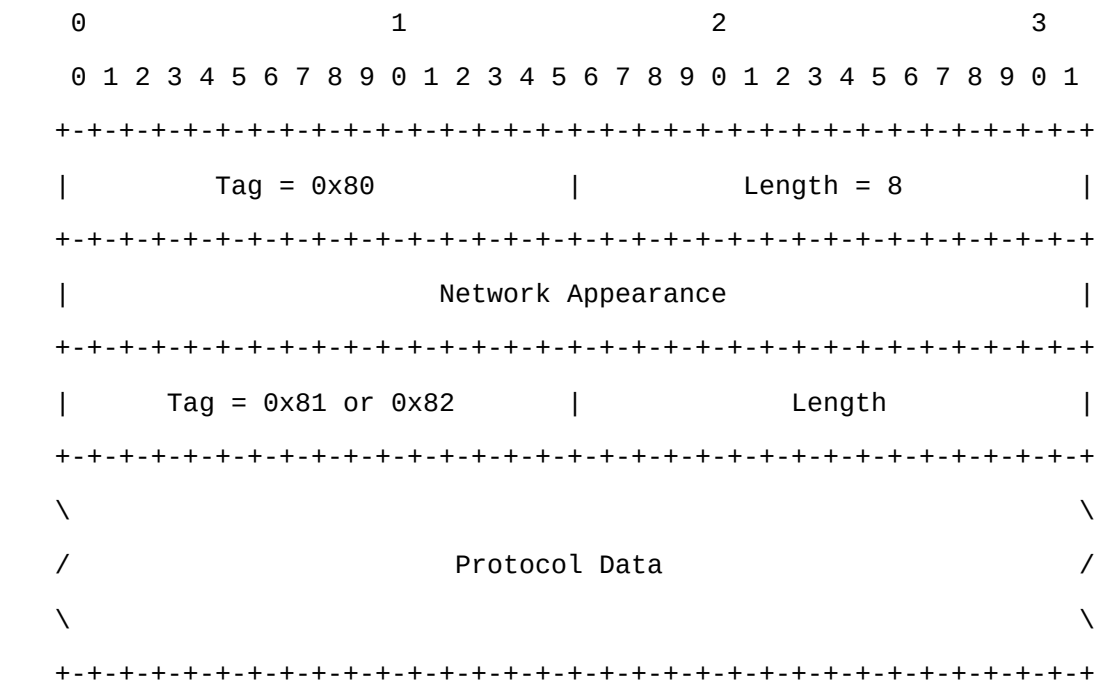
The following section describes the Transfer messages and parameter contents.

3.3.1 Payload Data Message (DATA)

The DATA message contains the SS7 MTP3-User protocol data, which is an MTP-TRANSFER primitive, including the complete MTP3 Routing Label. The DATA message contains the following variable length parameters:

Network Appearance	Optional
Protocol Data 1 or 2	Mandatory

The following format MUST be used for the Data Message:



Network Appearance: 32-bits (unsigned integer)

The optional Network Appearance parameter identifies the SS7 network context for the message, for the purposes of logically separating the signalling traffic between the SGP and the ASP over a common SCTP association. An example is where an SG is logically partitioned to appear as an element in four different national SS7 networks.

In a DATA message, the Network Appearance implicitly defines the SS7

Point Code format used, the SS7 Network Indicator value, and the MTP3 and possibly the MTP3-User protocol type/variant/version used within the SS7 network partition. Where an SG operates in the context of a single SS7 network, or individual SCTP associations are dedicated to each SS7 network context, the Network Appearance parameter is not required. In other cases the parameter MUST be included.

The Network Appearance parameter value is of local significance only, coordinated between the SGP and ASP. Therefore, in the case where an ASP is connected to more than one SGP, the same SS7 network context may be identified by different Network Appearance values depending over which SGP a message is being transmitted/received.

Where the optional Network Appearance parameter is present, it must be the first parameter in the message as it defines the format of the Protocol Data field

One of two possible Protocol Data parameters are included in a DATA message: Protocol Data 1 or Protocol Data 2.

Protocol Data 1 or 2: variable length

The Protocol Data 1 parameter contains the original SS7 MTP3 message, including the Service Information Octet and Routing Label.

The Protocol Data 1 parameter contains the following fields:

Service Information Octet. Includes:

Service Indicator,

Network Indicator,

and Spare/Priority codes.

Routing Label. Includes:

Destination Point Code,

Originating Point Code,

And Signalling Link Selection Code (SLS).

User Protocol Data. Includes:

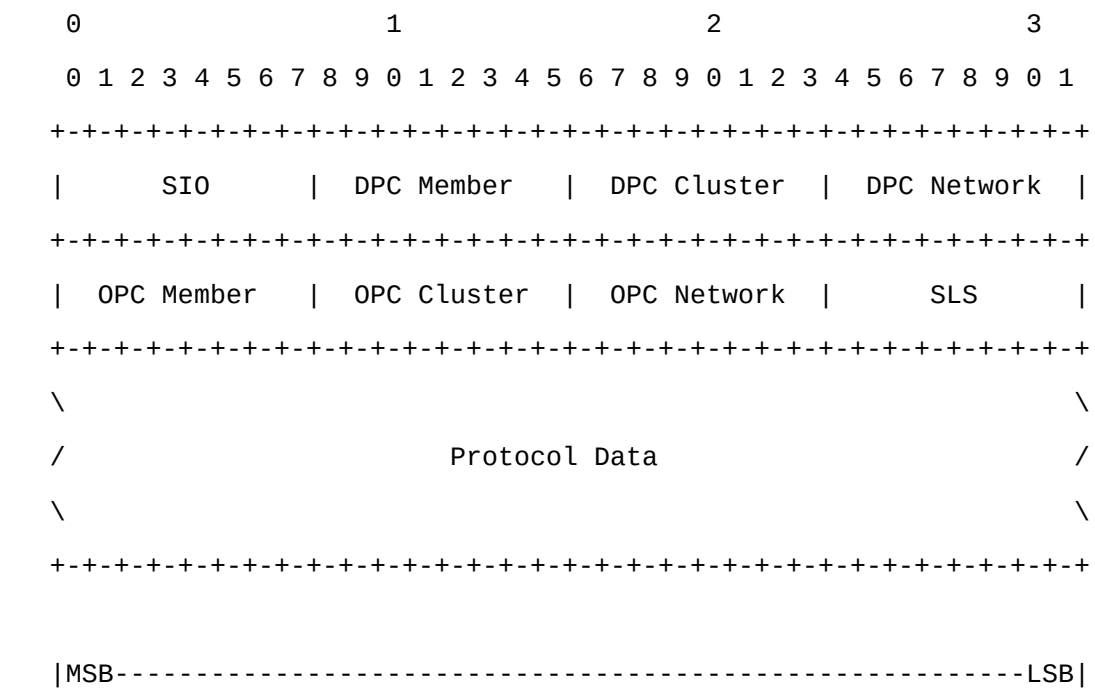
MTP3-User protocol elements (e.g., ISUP, SCCP, or TUP parameters).

The Protocol Data 2 parameter contains all the information in Protocol Data 1 as described above, plus the MTP2 Length Indicator octet. The MTP2 Length Indicator (LI) octet appears before the SIO and Routing Label information. The MTP2 Length Indicator octet is required for some national MTP variants that use the spare bits in the LI to carry additional information of interest to the MTP3 and MTP3-User (e.g., the Japan TTC standard use of LI spare bits to indicate message priority)

The Payload Data format is as defined in the relevant MTP standards for the SS7 protocol being transported. The format is either implicitly known or identified by the Network Appearance parameter. Note: In the SS7 Recommendations, the format of the messages and fields within the messages are based on bit transmission order. In these recommendations the Least Significant Bit (LSB) of each field is positioned to the right. The received SS7 fields are populated octet by octet as received into the 4-octet word as shown in the two examples below.

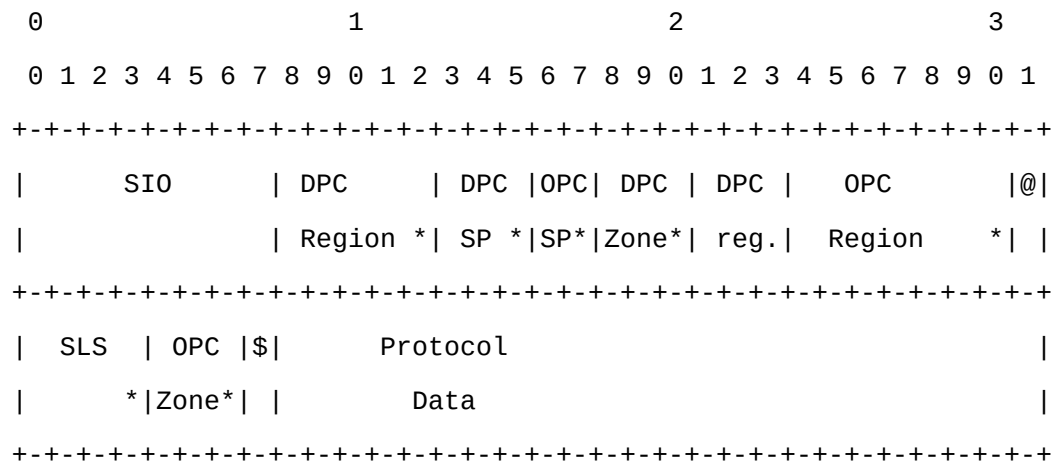
For the ANSI protocol example, the Protocol Data 1 field format is

shown below:



Within each octet the Least Significant Bit (LSB) per the SS7 Recommendations is to the right (e.g., bit 7 of SIO is the LSB).

For the ITU international protocol example (with the 3/8/3 Point Code format), the Protocol Data 1 field is shown below.



* marks LSB of each field; @ = OPC SP MSB; $ = OPC region MSB

3.4 SS7 Signalling Network Management (SSNM) Messages

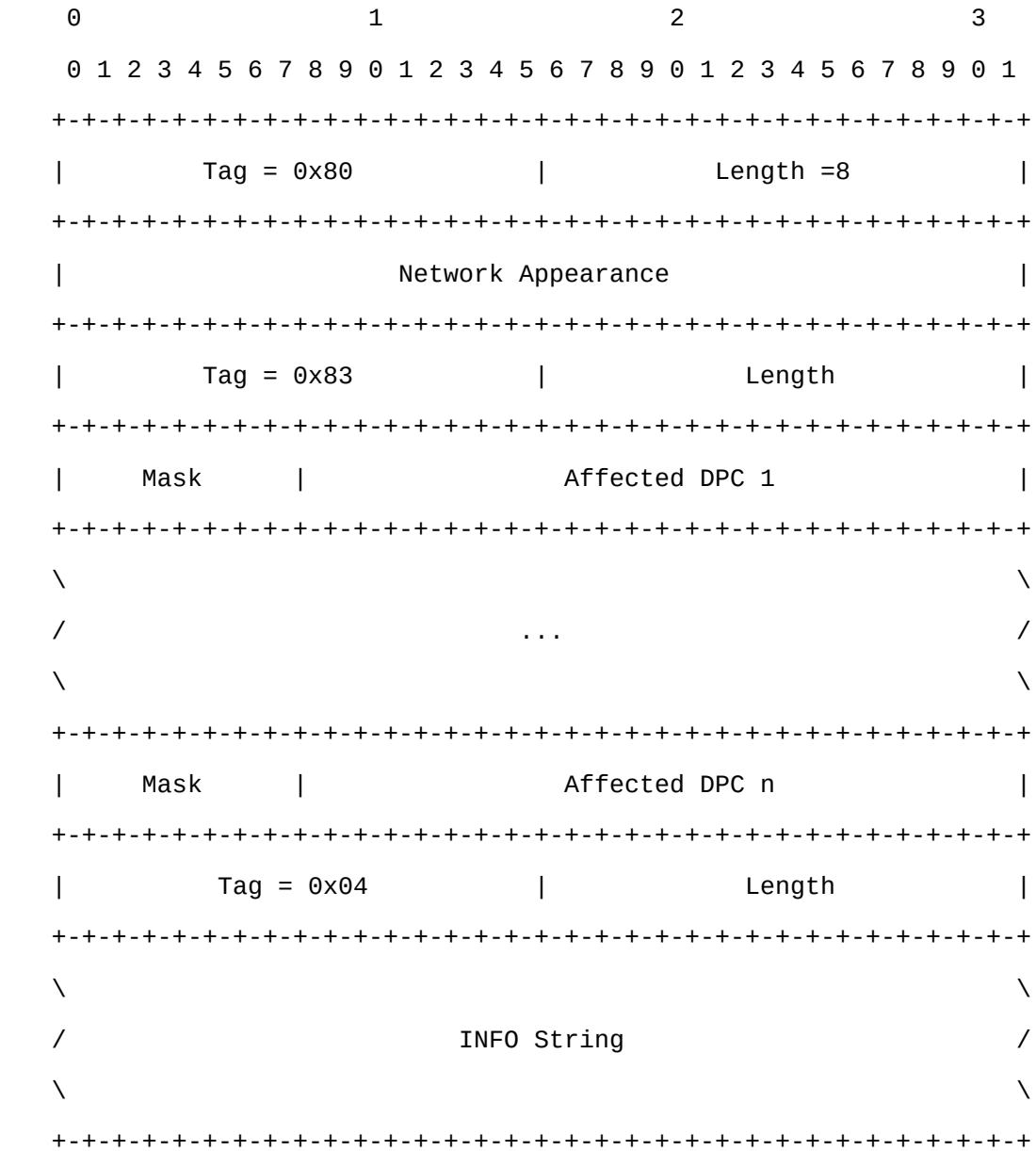
3.4.1 Destination Unavailable (DUNA)

The DUNA message is sent from all SGPs in an SG to all concerned ASPs to indicate that the SG has determined that one or more SS7 destinations are unreachable. It is also sent by an SGP in response to a message from the ASP to an unreachable SS7 destination. As an implementation option the SG may suppress the sending of subsequent "response" DUNA messages regarding a certain unreachable SS7 destination for a certain period in order to give the remote side time to react. The MTP3-User at the ASP is expected to stop traffic to the affected destination through the SGPs initiating the DUNA message as per the defined MTP3-User procedures.

The DUNA message contains the following parameters:

Network Appearance	Optional
Affected Destinations	Mandatory
INFO String	Optional

The format for DUNA Message parameters is as follows:



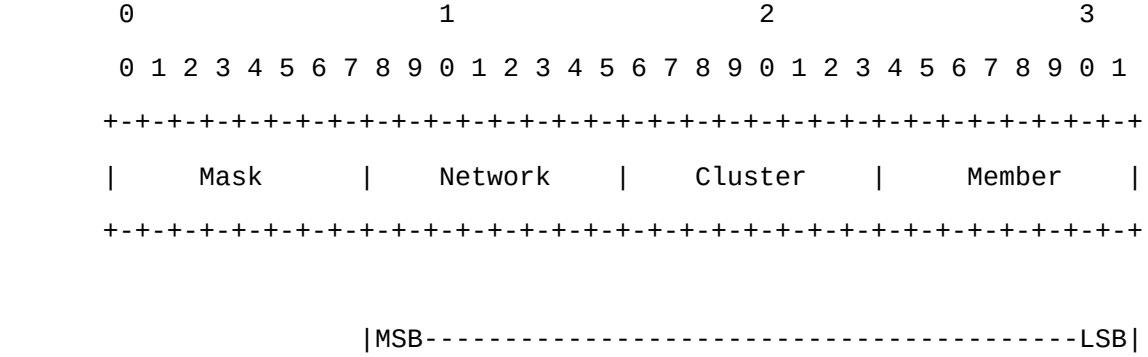
Network Appearance: 32-bit unsigned integer

See Section 3.3.1

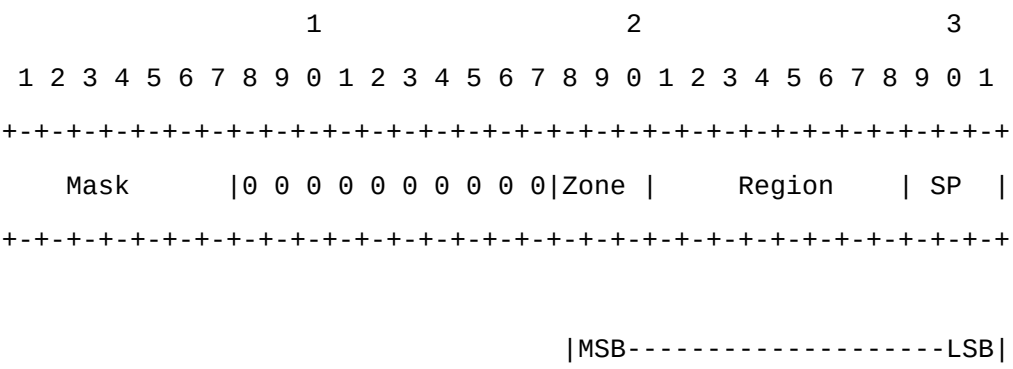
Affected Destinations: n x 32-bits

The Affected Destinations parameter contains up to sixteen Affected Destination Point Code fields, each a three-octet parameter to allow for 14-, 16- and 24-bit binary formatted SS7 Point Codes. Affected Point Codes that are less than 24-bits, are padded on the left to the 24-bit boundary. The encoding is shown below for ANSI and ITU Point Code examples.

ANSI 24-bit Point Code:



ITU 14-bit Point Code:



It is optional to send an Affected Destinations parameter with more than one Affected DPC but it is mandatory to receive and process it. All the Affected DPCs included must be within the same Network Appearance. Including multiple Affected DPCs may be useful when reception of an MTP3 management message or a linkset event simultaneously affects the availability status of a list of destinations at an SG.

Mask: 8-bits (unsigned integer)

The Mask field associated with each Affected DPC in the Affected Destinations parameter, used to identify a contiguous range of Affected Destination Point Codes, independent of the point code format. Identifying a contiguous range of Affected DPCs may be useful when reception of an MTP3 management message or a linkset event simultaneously affects the availability status of a series of destinations at an SG. For example, if all DPCs in an ANSI cluster are determined to be unavailable due to local linkset unavailability, the DUNA could identify potentially 256 Affected DPCs in a single Affected DPC field.

The Mask parameter represents a bit mask that can be applied to the related Affected DPC field. The bit mask identifies how many bits of the Affected DPC field are significant and which are effectively

"wildcarded". For example, a mask of "8" indicates that the least significant eight bits of the DPC is "wildcarded". For an ANSI 24-bit Affected DPC, this is equivalent to signalling that all DPCs in an ANSI Cluster are unavailable. A mask of "3" indicates that the least significant three bits of the DPC is "wildcarded". For a 14-bit ITU Affected DPC, this is equivalent to signaling that an ITU

Region is unavailable. A mask value equal to the number of bits in the DPC indicates that the entire network appearance is affected û this is used to indicate network isolation to the ASP.

INFO String: variable length

The optional INFO String parameter can carry any 8-bit ASCII character string along with the message. Length of the INFO String parameter is from 0 to 255 characters. No procedures are presently identified for its use but the INFO String MAY be used by Operators to identify in text form the location reflected by the Affected DPC for debugging purposes.

3.4.2 Destination Available (DAVA)

The DAVA message is sent from the SGP to all concerned ASPs to indicate that the SG has determined that one or more SS7 destinations are now reachable (and not restricted), or in response to a DAUD message if appropriate. The ASP MTP3-User protocol is informed and may now resume traffic to the affected destination. The ASP M3UA layer routes the MTP3_user traffic through the SGP(s) initiating the DAVA message.

The DAVA message contains the following parameters:

Network Appearance	Optional
Affected Destinations	Mandatory
INFO String	Optional

The format and description of the Network Appearance, Affected Destinations and INFO String parameters is the same as for the DUNA message (See Section 3.4.1).

3.4.3 Destination State Audit (DAUD)

The DAUD message MAY be sent from the ASP to the SGP to audit the availability/congestion state of SS7 routes to one or more affected destinations.

The DAUD message contains the following parameters:

Network Appearance	Optional
Affected Destinations	Mandatory
INFO String	Optional

The format and description of DAUD Message parameters is the same as for the DUNA message (See Section 3.4.1).

3.4.4 SS7 Network Congestion (SCON)

The SCON message can be sent from the SGP to all concerned ASPs to indicate congestion in the SS7 network to one or more destinations, or

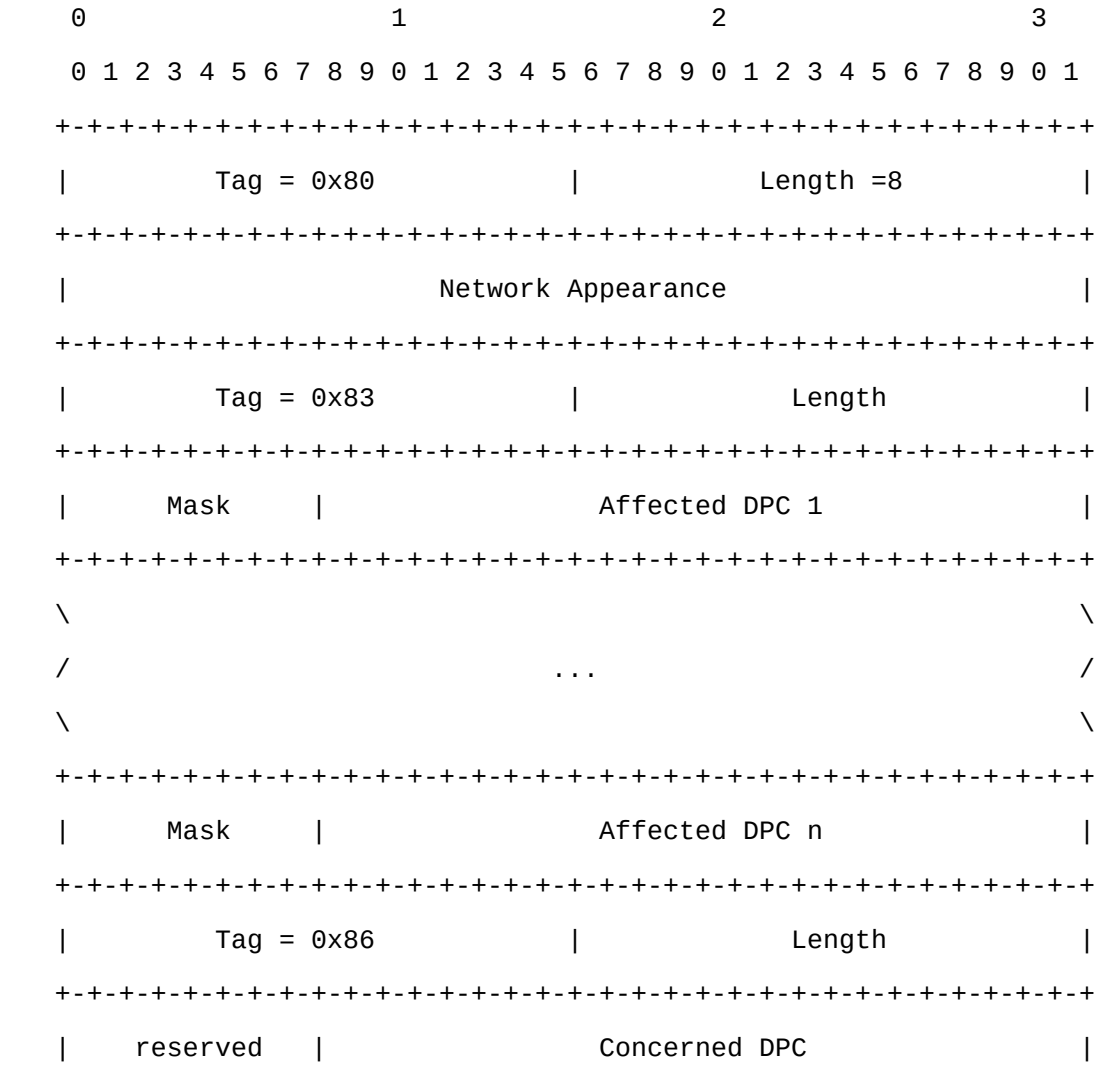
to an ASP in response to a DATA or DAUD message as appropriate. For

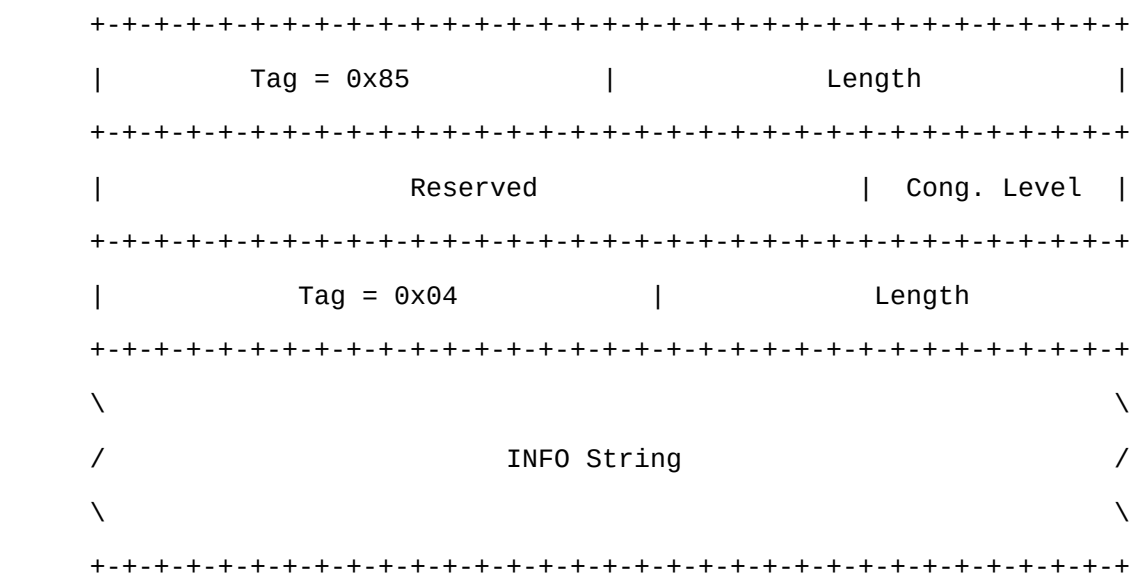
some MTP protocol variants (e.g., ANSI MTP) the SCON message may be sent when the SS7 congestion level changes. The SCON message MAY also be sent from the M3UA layer of an ASP to an M3UA peer indicating that the M3UA layer or the ASP is congested.

The SCON message contains the following parameters:

Network Appearance	Optional
Affected Destinations	Mandatory
Concerned Destination	Optional
Congestion Indications	Optional
INFO String	Optional

The format for SCON Message parameters is as follows:





The format and description of the Network Appearance, Affected Destinations, and INFO String parameters is the same as for the DUNA message (See Section 3.4.1).

The Affected Destinations parameter can be used to indicate congestion of multiple destinations or ranges of destinations. However, an SCON message MUST not be delayed in order to "collect" individual congested destinations into a single SCON message as any delay might affect the timing of congestion indications to the M3UA Users. One use for including a range of Congested DPCs is when the SG supports an ANSI cluster route set to the SS7 network that becomes congested due to outgoing link set congestion.

Concerned Destination: 32-bits

The optional Concerned Destination parameter is only used if the SCON message is sent from an ASP to the SGP. It contains the point code of the originator of the message that triggered the SCON

message. The Concerned Destination parameter contains one Concerned Destination Point Code field, a three-octet parameter to allow for 14-, 16- and 24-bit binary formatted SS7 Point Codes. A Concerned Point Code that is less than 24-bits is padded on the left to the 24-bit boundary. Any resulting Transfer Controlled (TFC) message from the SG is sent to the Concerned Point Code using the single Affected DPC contained in the SCON message to populate the (affected) Destination field of the TFC message

Congested Indications: 32-bits

The optional Congestion Indications parameter contains a Congestion Level field. This optional parameter is used to communicate congestion levels in national MTP networks with multiple congestion thresholds, such as in ANSI MTP3. For MTP congestion methods without multiple congestion levels (e.g., the ITU international method) the parameter is not included.

Congestion Level field: 8-bits (unsigned integer)

The Congestion Level field, associated with all of the Affected DPC(s) in the Affected Destinations parameter, contains one of the Following values:

0	No Congestion or Undefined
1	Congestion Level 1
2	Congestion Level 2
3	Congestion Level 3

The congestion levels are defined in the congestion method in the appropriate national MTP recommendations [14,15].

3.4.5 Destination User Part Unavailable (DUPU)

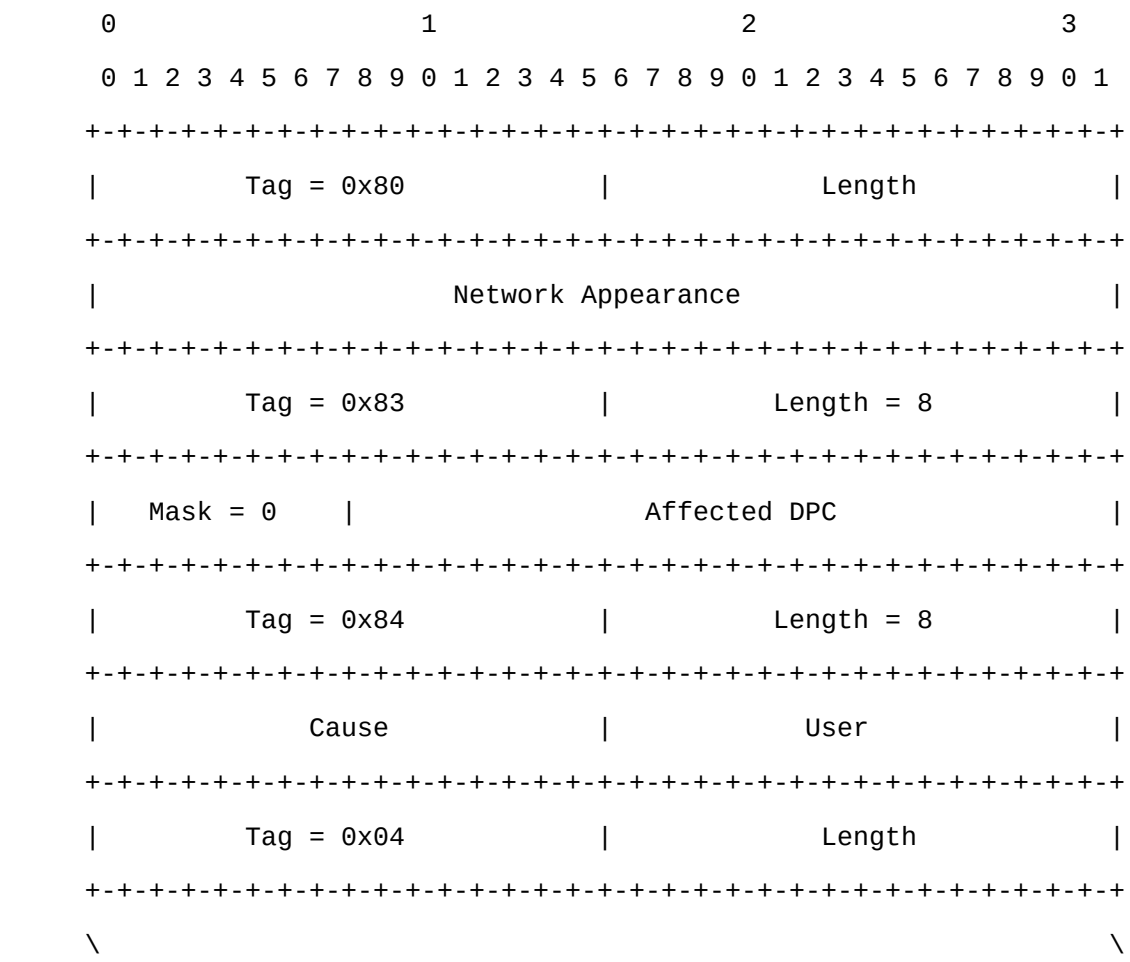
The DUPU message is used by an SGP to inform an ASP that a remote peer

MTP3-User Part (e.g., ISUP or SCCP) at an SS7 node is unavailable.

The DUPU message contains the following parameters:

Network Appearance	Optional
Affected Destinations	Mandatory
User/Cause	Mandatory
INFO String	Optional

The format for DUPU message parameters is as follows:



```
   /                          INFO String                          /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

User/Cause: 32-bits

The Unavailability Cause and MTP3-User Identity fields, associated with the Affected DPC in the Affected Destinations parameter, are encoded as follows:

Unavailability Cause field: 16-bits (unsigned integer)

The Unavailability Cause parameter provides the reason for the unavailability of the MTP3-User. The valid values for the Unavailability Cause parameter are shown in the following table. The values agree with those provided in the SS7 MTP3 User Part Unavailable message. Depending on the MTP3 protocol used in the Network Appearance, additional values may be used - the specification of the relevant MTP3 protocol variant/version recommendation is definitive.

0	Unknown
1	Unequipped Remote User
2	Inaccessible Remote User

MTP3-User Identity field: 16-bits (unsigned integer)

The MTP3-User Identity describes the specific MTP3-User that is unavailable (e.g., ISUP, SCCP, ...). Some of the valid values for the MTP3-User Identity are shown below. The values align with those

provided in the SS7 MTP3 User Part Unavailable message and Service Indicator. Depending on the MTP3 protocol variant/version used in the network appearance, additional values may be used. The relevant MTP3 protocol variant/version recommendation is definitive.

0 to 2	Reserved
3	SCCP
4	TUP
5	ISUP
6 to 8	Reserved
9	Broadband ISUP
10	Satellite ISUP
11	Reserved
12	AAL type 2 Signalling
13	Bearer Independent Call Control (BICC)
14	Gateway Control Protocol
15	Reserved

The format and description of the Affected Destinations parameter is the same as for the DUNA message (See Section 3.4.1.) except that the Mask field is not used and only a single Affected DPC is included. Ranges and lists of Affected DPCs cannot be signalled in a DUPU message, but this is consistent with UPU operation in the SS7 network. The Affected Destinations parameter in an MTP3 User Part Unavailable message (UPU) received by an SGP from the SS7 network contains only one destination.

The format and description of the Network Appearance and INFO String parameters is the same as for the DUNA message (See Section 3.4.1).

3.4.6 Destination Restricted (DRST)

The DRST message is optionally sent from the SGP to all concerned ASPs

to indicate that the SG has determined that one or more SS7 destinations are now restricted from the point of view of the SGP, or in response to a DAUD message if appropriate. The M3UA layer at the ASP is expected to send traffic to the affected destination via an alternate SGP of equal priority, but only if such an alternate route exists and is available. If the affected destination is currently considered unavailable by the ASP, The MTP3-User should be informed that traffic to the affected destination can be resumed. In this case, the M3UA layer should route the traffic through the SGP initiating the DRST message.

This message is optional for the SGP to send and it is optional for the ASP to act on any information received in the message. It is for use in the "STP" case described in Section 1.4.1.

The DRST message contains the following parameters:

Network Appearance	Optional
Affected Destinations	Mandatory
INFO String	Optional

The format and description of the Network Appearance, Affected Destinations and INFO String parameters is the same as for the DUNA message (See Section 3.4.1).

3.5 ASP State Maintenance (ASPSM) Messages

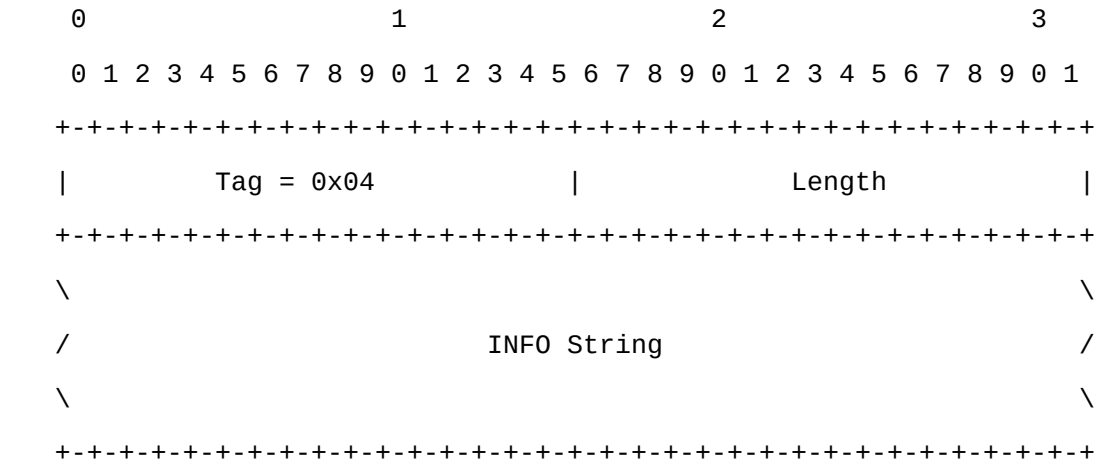
3.5.1 ASP Up

The ASP Up message is used to indicate to a remote M3UA peer that the adaptation layer is ready to receive any SSNM or ASPSM/ASPTM messages for all Routing Keys that the ASP is configured to serve.

The ASP Up message contains the following parameters:

INFO String Optional

The format for ASP Up message parameters is as follows:



The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1).

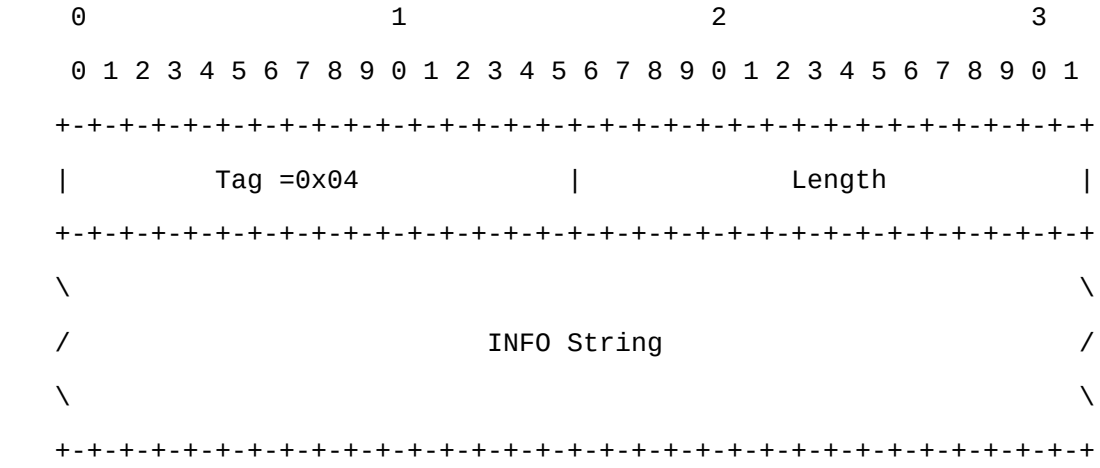
3.5.2 ASP Up Acknowledgement (ASP Up Ack)

The ASP UP Ack message is used to acknowledge an ASP Up message received from a remote M3UA peer.

The ASP Up Ack message contains the following parameters:

INFO String (optional)

The format for ASP Up Ack message parameters is as follows:



The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1). The INFO String in an ASP Up Ack message is independent from the INFO String in the ASP Up message (i.e., it does not have to echo back the INFO String received).

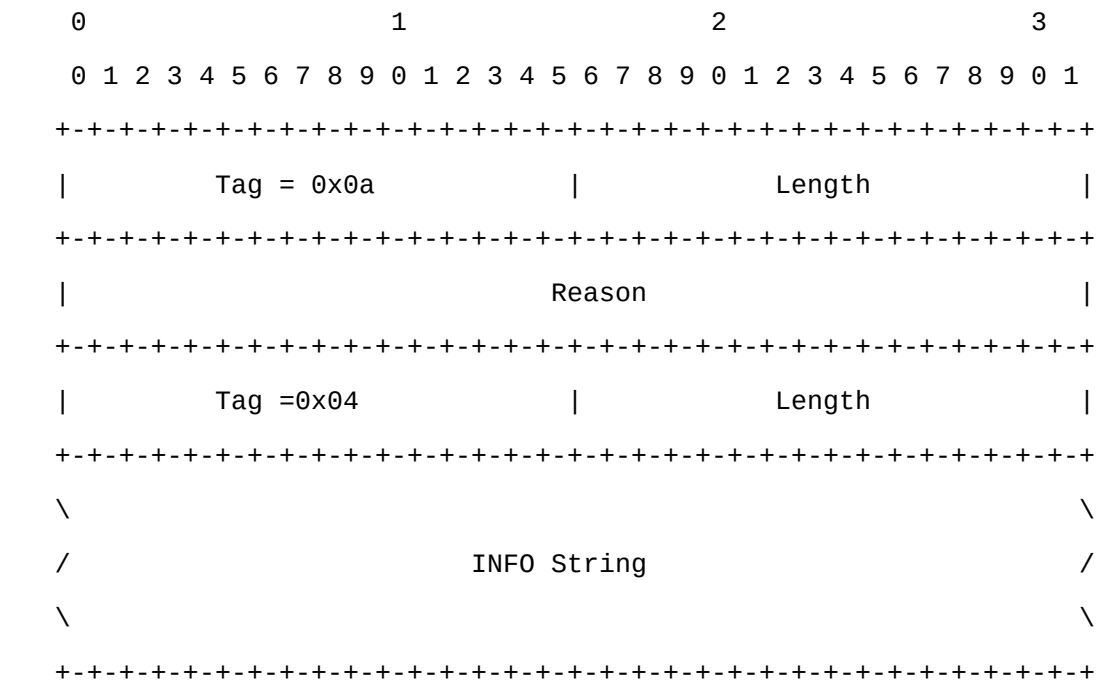
3.5.3 ASP Down

The ASP Down message is used to indicate to a remote M3UA peer that the adaptation layer is NOT ready to receive DATA, SSNM or ASPTM messages.

The ASP Down message contains the following parameters:

Reason	Mandatory
INFO String	Optional

The format for the ASP Down message parameters is as follows:



The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1).

Reason: 32-bit (unsigned integer)

The Reason parameter indicates the reason that the remote M3UA adaptation layer is unavailable. The valid values for Reason are shown in the following table.

0	Unspecified
1	User Unavailable
2	Management Blocking

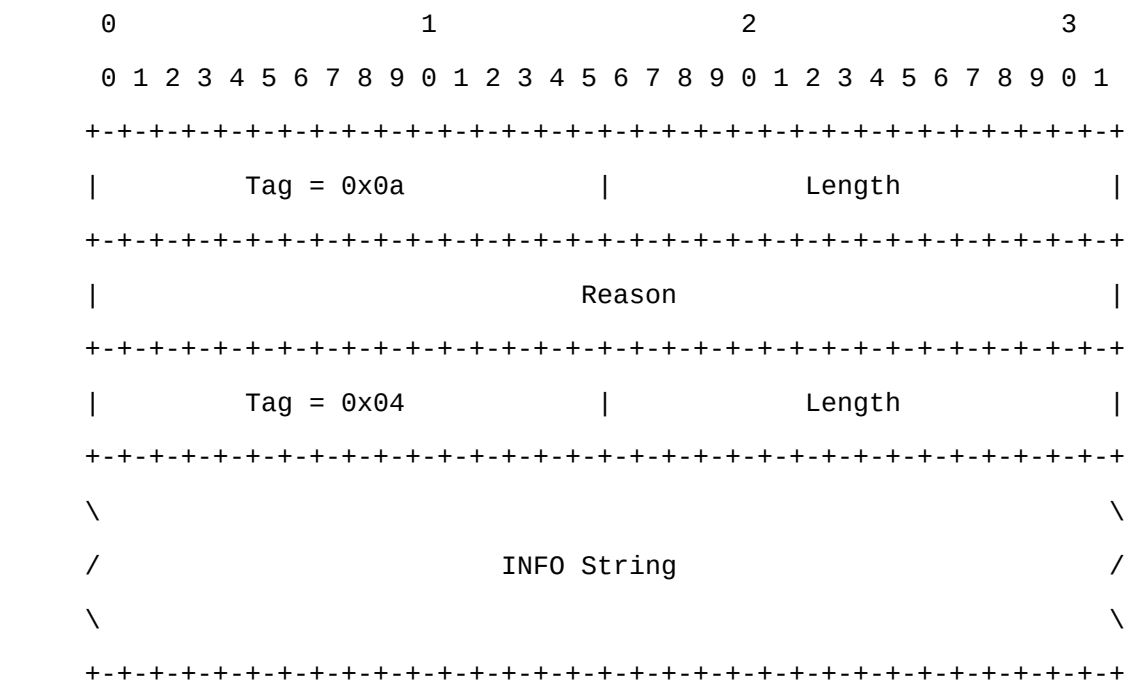
3.5.4 ASP Down Acknowledgement (ASP Down Ack)

The ASP Down Ack message is used to acknowledge an ASP Down message received from a remote M3UA peer.

The ASP Down Ack message contains the following parameters:

Reason	Mandatory
INFO String	Optional

The format for the ASP Down Ack message parameters is as follows:



The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1).

The INFO String in an ASP Down Ack message is independent from the INFO

String in the ASP Down message (i.e., it does not have to echo back the INFO String received).

The format of the Reason parameter is the same as for the ASP-Down message. (See Section 3.5.3).

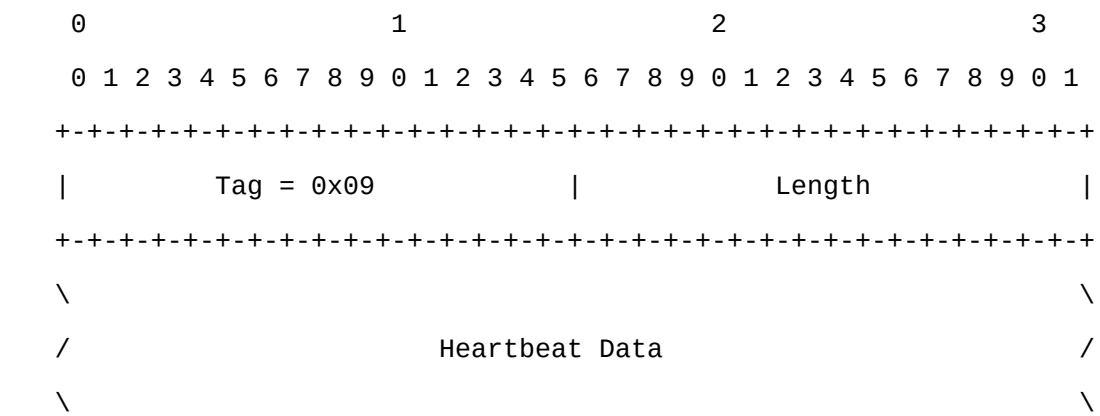
3.5.5 Heartbeat (BEAT)

The BEAT message is optionally used to ensure that the M3UA peers are still available to each other. It is recommended for use when the M3UA runs over a transport layer other than the SCTP, which has its own heartbeat.

The BEAT message contains the following parameters:

Heatbeat Data Optional

The format for the BEAT message is as follows:



The Heartbeat Data parameter contents are defined by the sending node. The Heartbeat Data could include, for example, a Heartbeat Sequence Number and/or Timestamp. The receiver of a BEAT message does not process this field as it is only of significance to the sender. The receiver MUST respond with a BEAT Ack message.

3.5.6 Heartbeat Acknowledgement (BEAT Ack)

The BEAT Ack message is sent in response to a received BEAT message. It includes all the parameters of the received BEAT message, without any change.

3.6 Routing Key Management (RKM) Messages

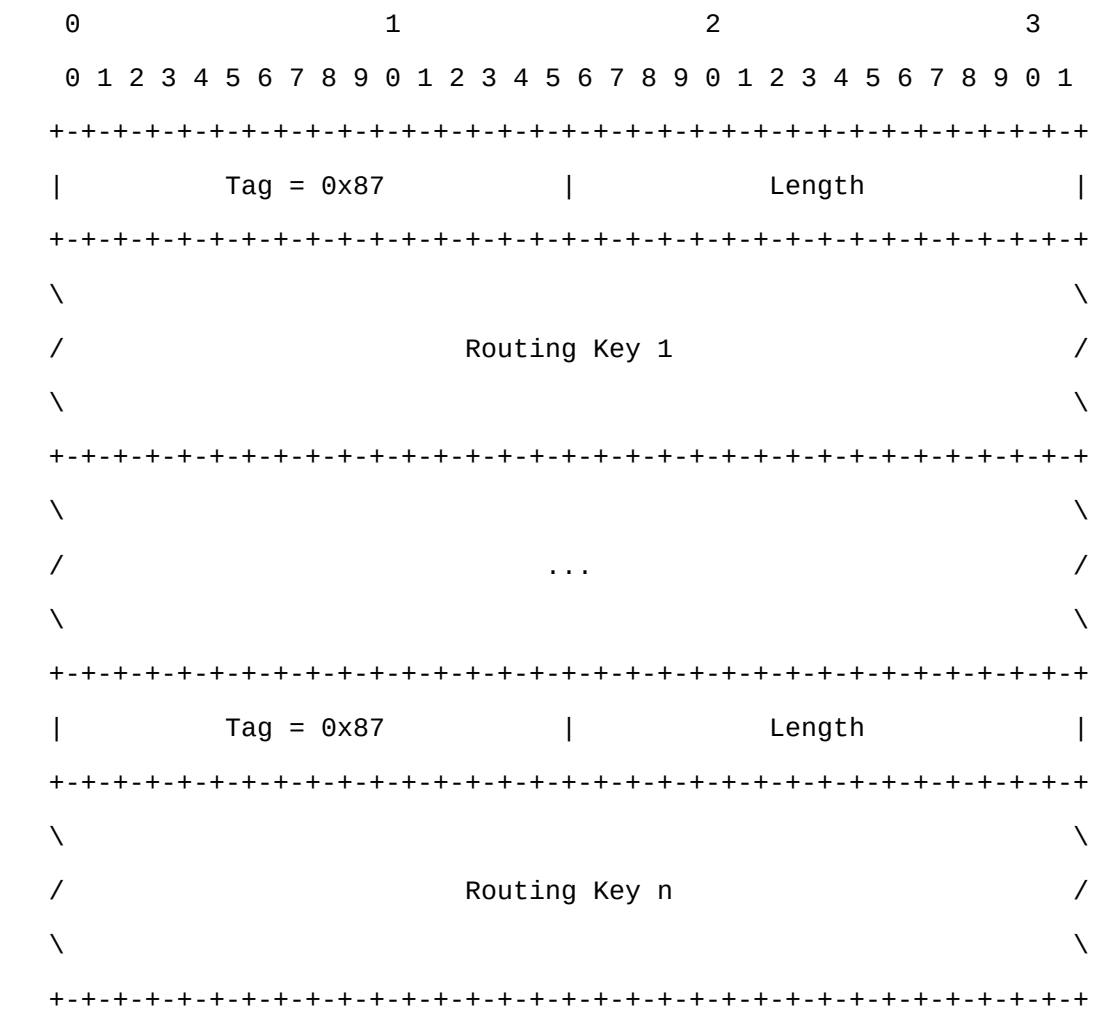
3.6.1 Registration Request (REG REQ)

The REG REQ message is sent by an ASP to indicate to a remote M3UA peer that it wishes to register one or more given Routing Keys with the remote peer. Typically, an ASP would send this message to an SGP, and expects to receive a REG RSP message in return with an associated Routing Context value.

The REG REQ message contains the following parameters:

Routing Key	Mandatory

The format for the REG REQ message is as follows:

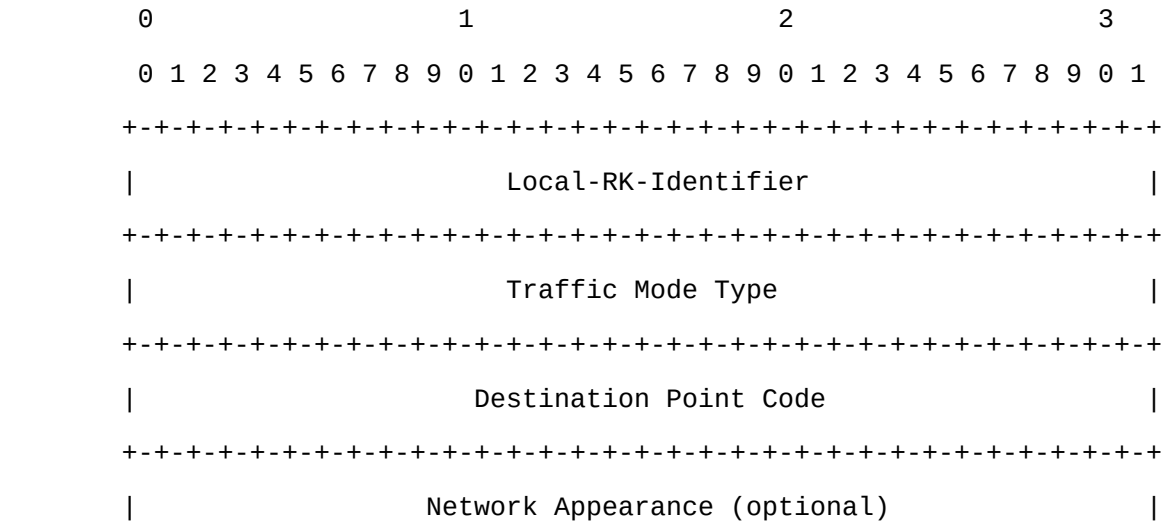


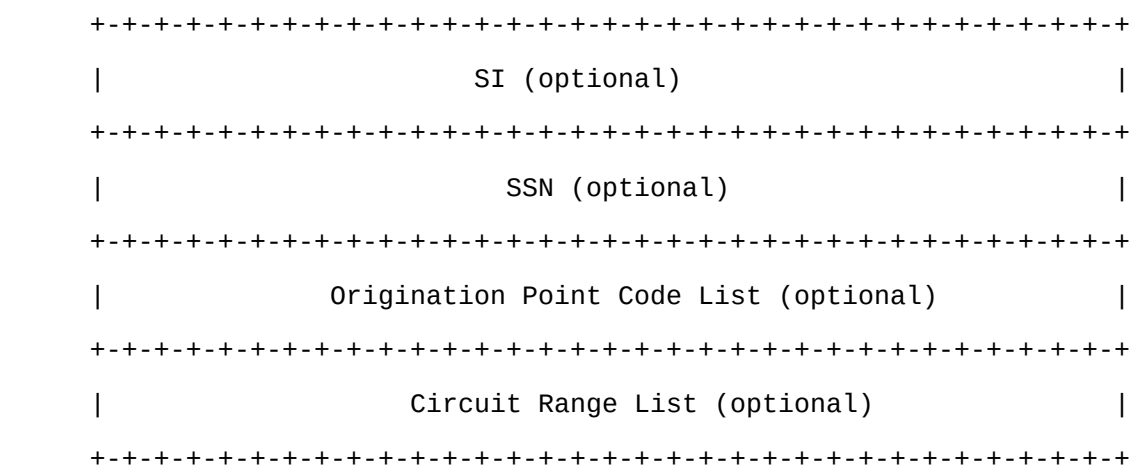
Routing Key: variable length

The Routing Key parameter is mandatory. The sender of this message expects that the receiver of this message will create a Routing Key entry and assign a unique Routing Context value to it, if the Routing Key entry does not already exist.

The Routing Key parameter may be present multiple times in the same message. This is used to allow the registration of multiple Routing Keys in a single message.

The format of the Routing Key parameter is as follows.

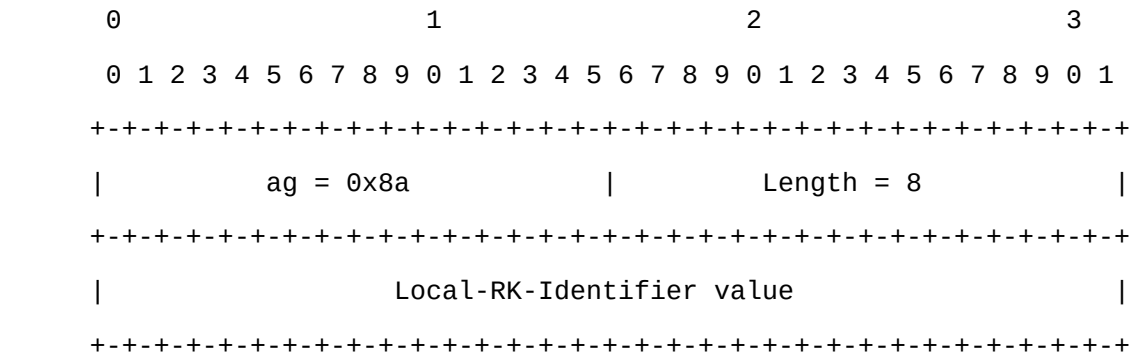




Local-RK-Identifier: 32-bit integer

The mandatory Local-RK-Identifier field is used to uniquely identify the registration request. The Identifier value is assigned by the ASP, and is used to correlate the response in an REG RSP message with the original registration request. The Identifier value must remain unique until the REG RSP message is received.

The format of the Local-RK-Identifier field is as follows:



Traffic Mode Type: 32-bit (unsigned integer)

The Traffic Mode Type parameter is mandatory and identifies the traffic mode of operation of the ASP(s) within an Application Server. The valid values for Traffic Mode Type are shown in the following table:

1 Over-ride

2 Load-share

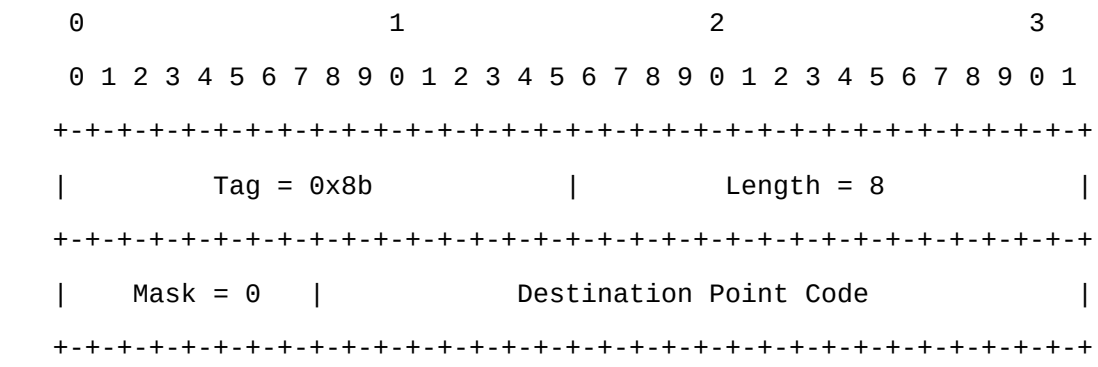
Sidebottom et al [Page 48]

Internet Draft SS7 MTP3-User Adaptation Layer Jul 2001

If the receiver of the REG REQ creates a new Routing Key entry, then the Traffic Mode Type sets the traffic mode for the new Application Server. If the receiver of the REG REQ determines that a matching Routing Key already exists, the Traffic Mode Type MUST match the existing traffic mode for the AS.

Destination Point Code:

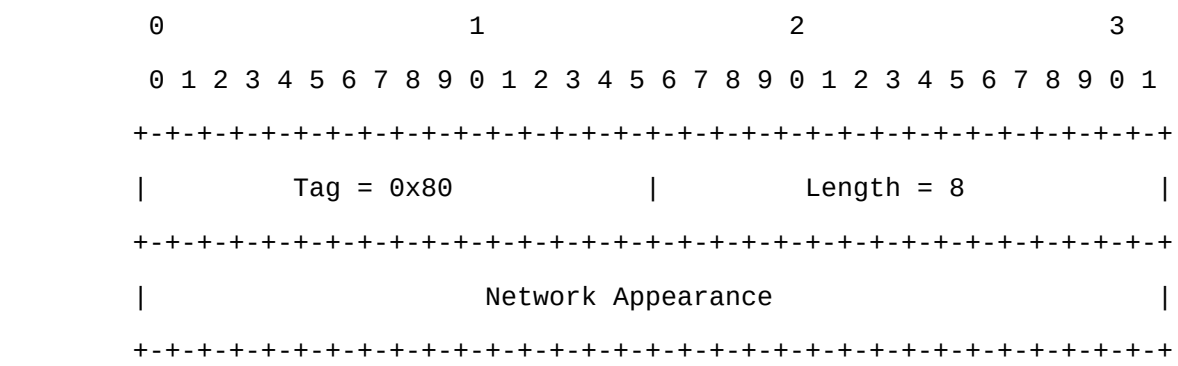
The Destination Point Code parameter is mandatory, and identifies the Destination Point Code of incoming SS7 traffic for which the ASP is registering. The format is the same as described for the Affected Destination parameter in the DUNA message (See Section 3.4.1). Its format is:



Network Appearance:

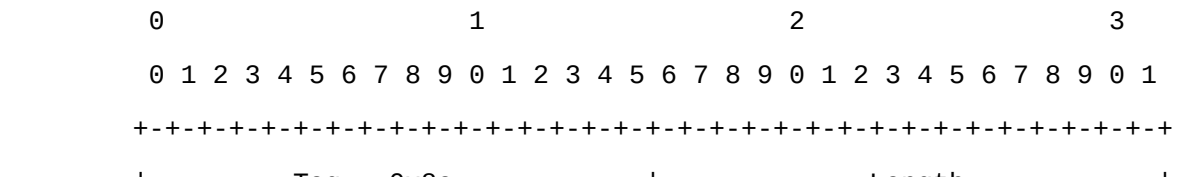
The optional Network Appearance parameter field identifies the SS7 network context for the Routing Key, and has the same format as in

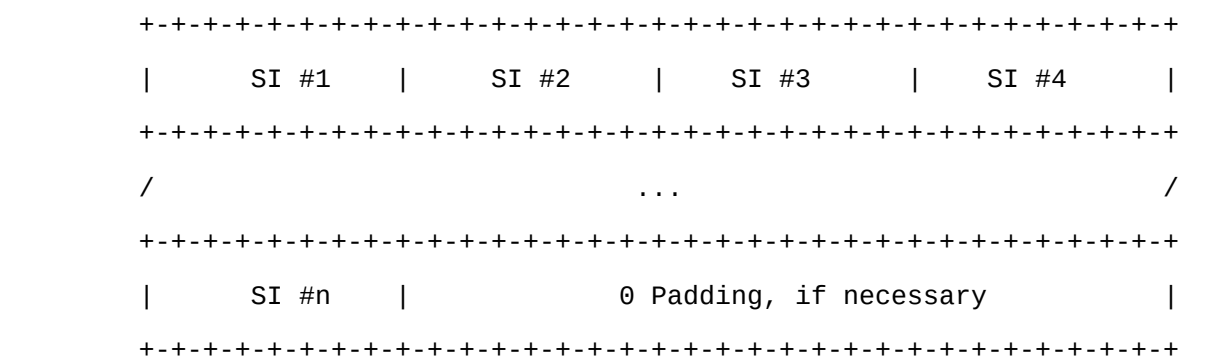
the DATA message (See Section 3.3.1). The absence of the Network Appearance parameter in the Routing Key indicates the use of any Network Appearance value, Its format is:



Service Indicators (SI): n X 8-bit integers

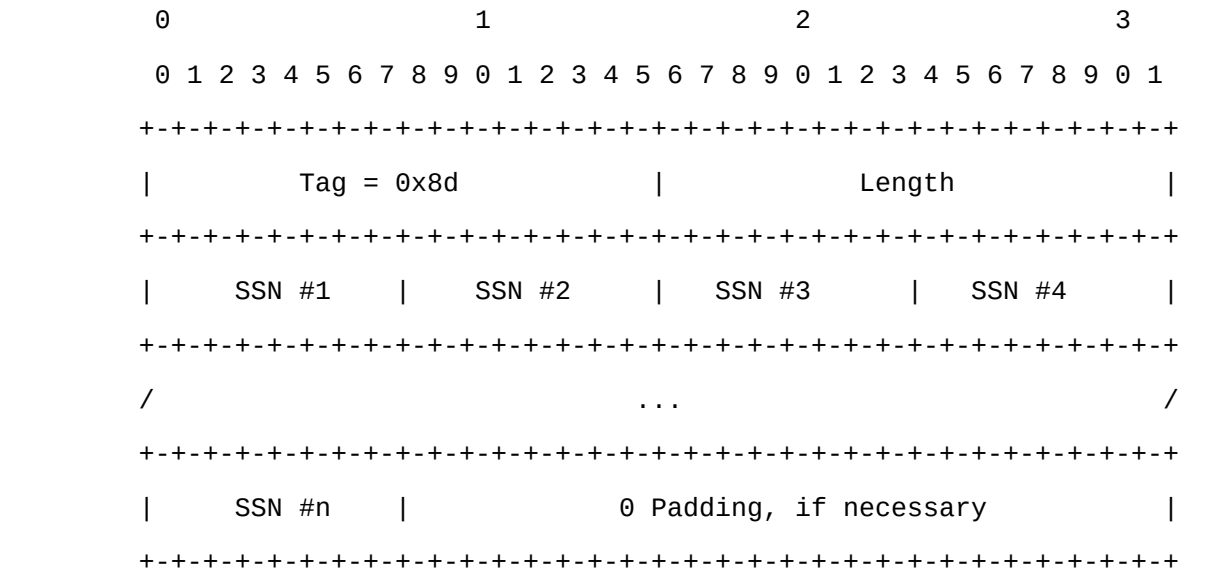
The optional SI field contains one or more Service Indicators from the values as described in the MTP3-User Identity field of the DUPU message. The absence of the SI parameter in the Routing Key indicates the use of any SI value, excluding of course MTP management. Where an SI parameter does not contain a multiple of four SIs, the parameter is padded out to 32-byte alignment. An SI value of zero is not valid in M3UA. The SI format is:





Subsystem Numbers (SSN): n X 8-bit integers

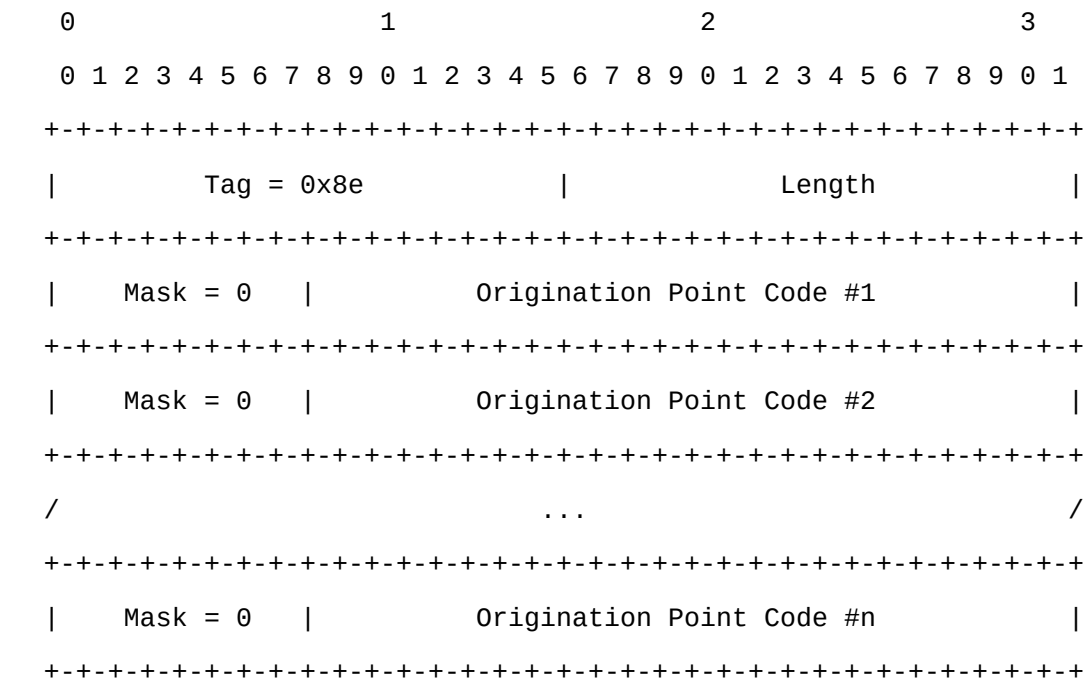
The optional SSN field contains one or more SCCP subsystem numbers, and is used in conjunction with an SI values of 3 (i.e., SCCP) only. The absence of the SSN parameter in the Routing Key indicates the use of any SSN value, in the case of SCCP traffic. Where an SSN parameter does not contain a multiple of four SSNs, the parameter is padded out to 32-byte alignment. The subsystem number values associated are defined by the local network operator, and typically follow ITU-T Recommendation Q.713 [5]. An SSN value of zero is not valid in M3UA. The format of this field is as follows:



OPC List:

The Originating Point Code List parameter contains one or more SS7

OPC entries, and its format is the same as the Destination Point Code parameter. The absence of the OPC List parameter in the Routing Key indicates the use of any OPC value,

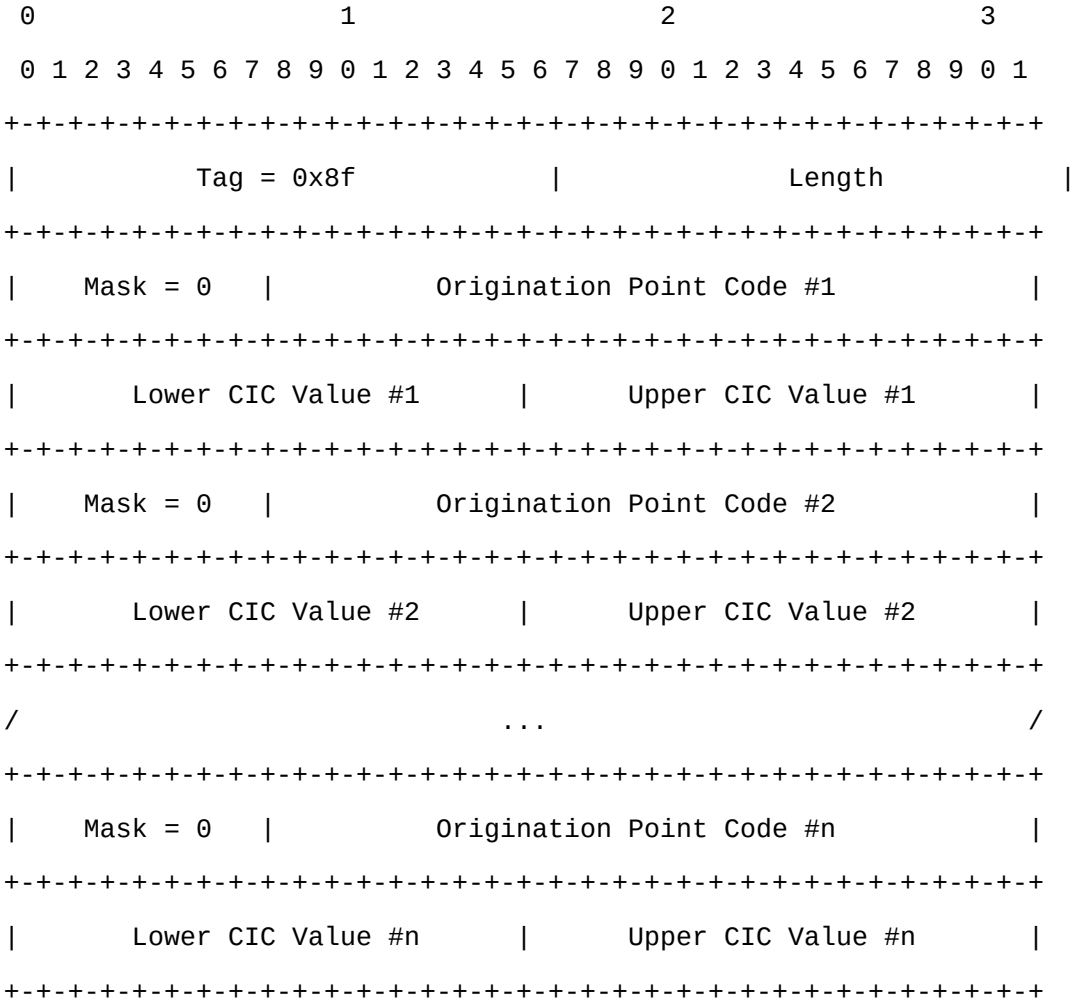


Circuit Range:

An ISUP controlled circuit is uniquely identified by the SS7 OPC,

DPC and CIC value. For the purposes of identifying Circuit Ranges in an M3UA Routing Key, the optional Circuit Range parameter includes one or more circuit ranges, each identified by an OPC and Upper/Lower CIC value. The DPC is implicit as it is mandatory and already included in the DPC parameter of the Routing Key. The absence of the Circuit Range parameter in the Routing Key indicates the use of any Circuit Range values, in the case of ISUP/TUP traffic. The Origination Point Code is encoded the same as the Destination Point Code parameter, while the CIC values are 16-bit integers.

The Circuit Range format is as follows:



Sidebottom et al [Page 51]

Internet Draft SS7 MTP3-User Adaptation Layer Jul 2001

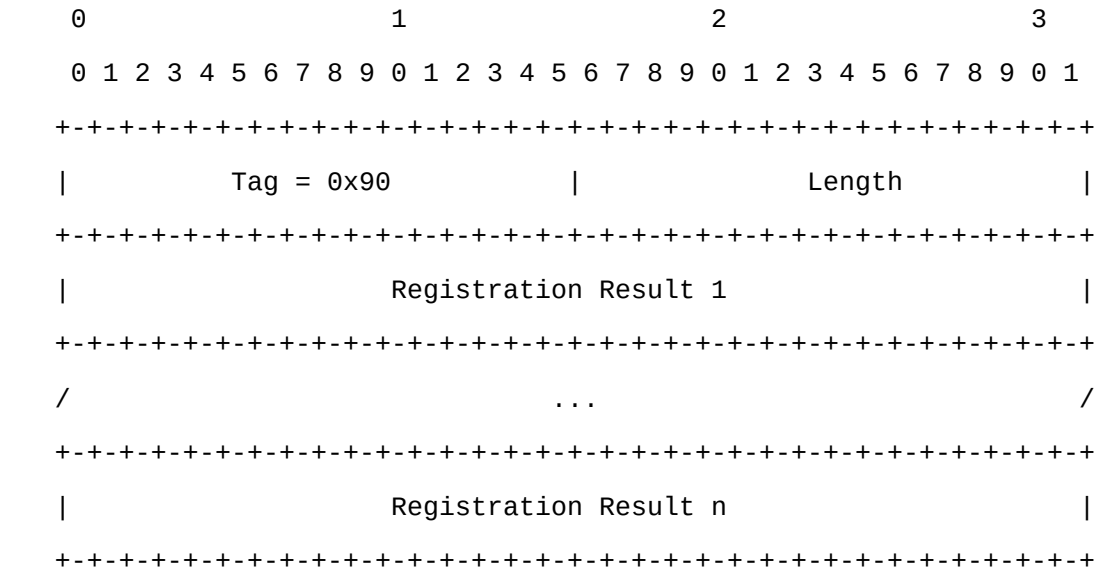
3.6 2 Registration Response (REG RSP)

The REG RSP message is used as a response to the REG REQ message from a remote M3UA peer. It contains indications of success/failure for registration requests and returns a unique Routing Context value for successful registration requests, to be used in subsequent M3UA Traffic Management protocol.

The REG RSP message contains the following parameters:

Registration Results Mandatory

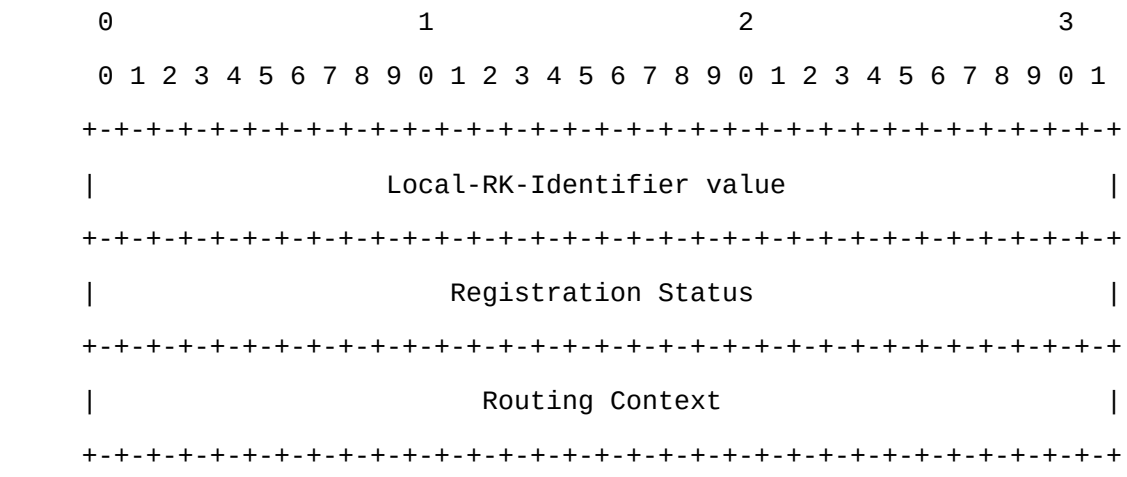
The format for the REG RSP message is as follows:



Registration Results:

The Registration Results parameter contains one or more results, each containing the registration status for a single Routing Key in

an REG REQ message. The number of results in a single REG RSP message MAY match the number of Routing Key parameters found in the corresponding REG REQ message. The format of each result is as follows:



Local-RK-Identifier: 32-bit integer

The Local-RK-Identifier contains the same value as found in the matching Routing Key parameter found in the REG REQ message (See Section 3.5.5.1).

Registration Status: 32-bit integer

The Registration Result Status field indicates the success or the reason for failure of a registration request.

Its values may be:

0	Successfully Registered
1	Error - Unknown
2	Error - Invalid DPC
3	Error - Invalid Network Appearance
4	Error - Invalid Routing Key
5	Error - Permission Denied
6	Error - Cannot Support Unique Routing
7	Error - Routing Key not Currently Provisioned
8	Error - Insufficient Resources
9	Error - Unsupported RK parameter Field
10	Error û Unsupported/Invalid Traffic Handling Mode

Routing Context: 32-bit integer

The Routing Context field contains the Routing Context value for the associated Routing Key if the registration was successful. It is set to "0" if the registration was not successful.

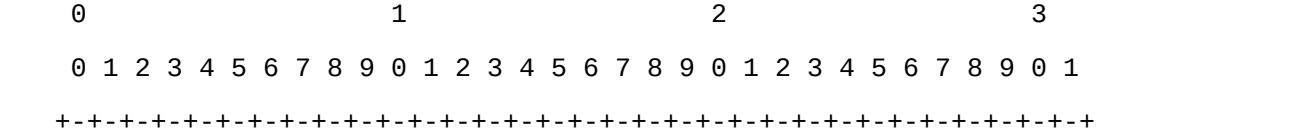
3.6.3 De-Registration Request (DEREG REQ)

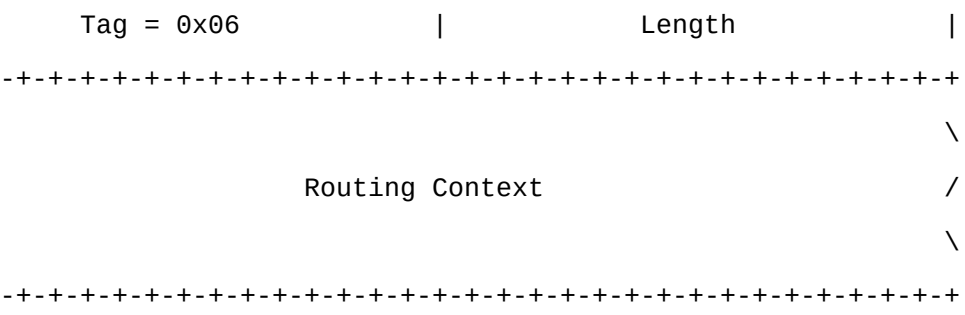
The DEREG REQ message is sent by an ASP to indicate to a remote M3UA peer that it wishes to de-register a given Routing Key. Typically, an ASP would send this message to an SGP, and expects to receive a DEREG RSP message in return with the associated Routing Context value.

The DEREG REQ message contains the following parameters:

Routing Context	Mandatory

The format for the DEREG REQ message is as follows:





Routing Context: n X 32-bit integers

The Routing Context parameter contains (a list of) integers indexing the Application Server traffic that the sending ASP is currently registered to receive from the SGP but now wishes to deregister.

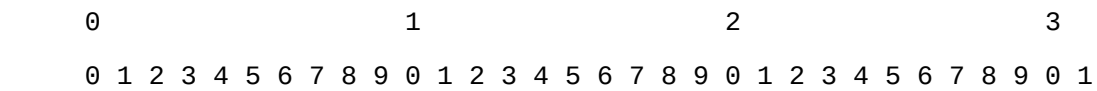
3.6.4 De-Registration Response (DEREG RSP)

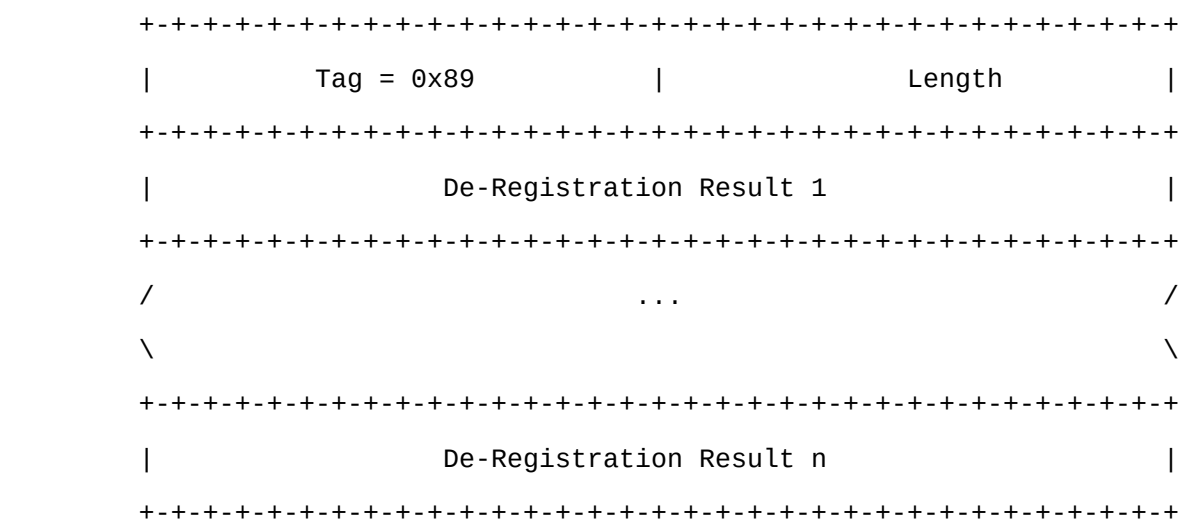
The DEREG RSP message is used as a response to the DEREG REQ message from a remote M3UA peer.

The DEREG RSP message contains the following parameters:

De-registration Results Mandatory

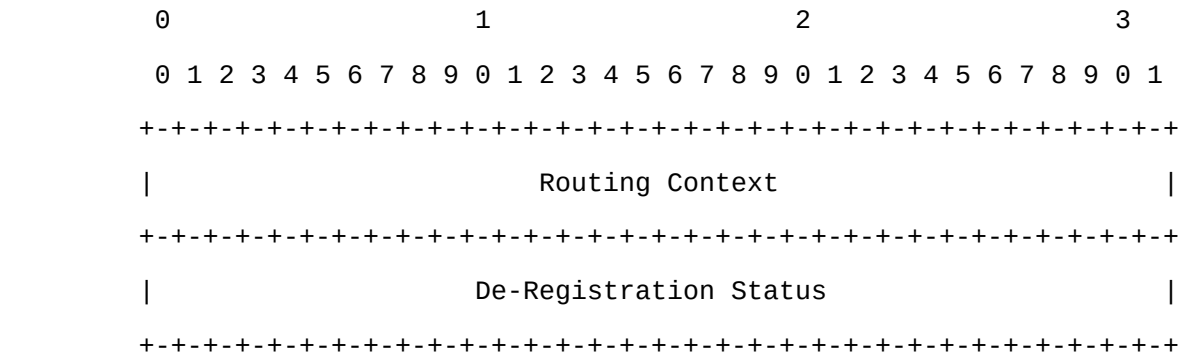
The format for the DEREG RSP message is as follows:





De-Registration Results:

The De-Registration Results parameter contains one or more results, each containing the de-registration status for a single Routing Context in a DEREG REQ message. The number of results in a single DEREG RSP message MAY match the number of Routing Contexts found in the corresponding DEREG REQ message. The format of each result is as follows:



Routing Context: 32-bit integer

The Routing Context field contains the Routing Context value of the matching Routing Key to deregister, as found in the DEREG REQ message.

De-Registration Status: 32-bit integer

The De-Registration Result Status field indicates the success or the reason for failure of the de-registration.

Its values may be:

0	Successfully De-registered
1	Error - Unknown
2	Error - Invalid Routing Context
3	Error - Permission Denied
4	Error - Not Registered
5	Error û ASP Currently Active for Routing Context

3.7 ASP Traffic Maintenance (ASPTM) Messages

3.7.1 ASP Active

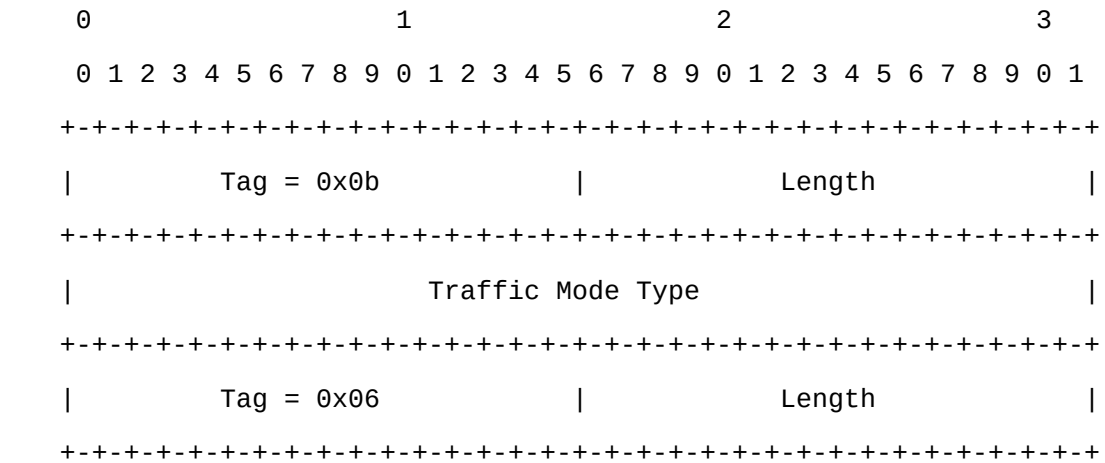
The ASP Active message is sent by an ASP to indicate to a remote M3UA peer that it is ready to process signalling traffic for a particular Application Server. The ASP Active message affects only the ASP state for the Routing Keys identified by the Routing Contexts, if present.

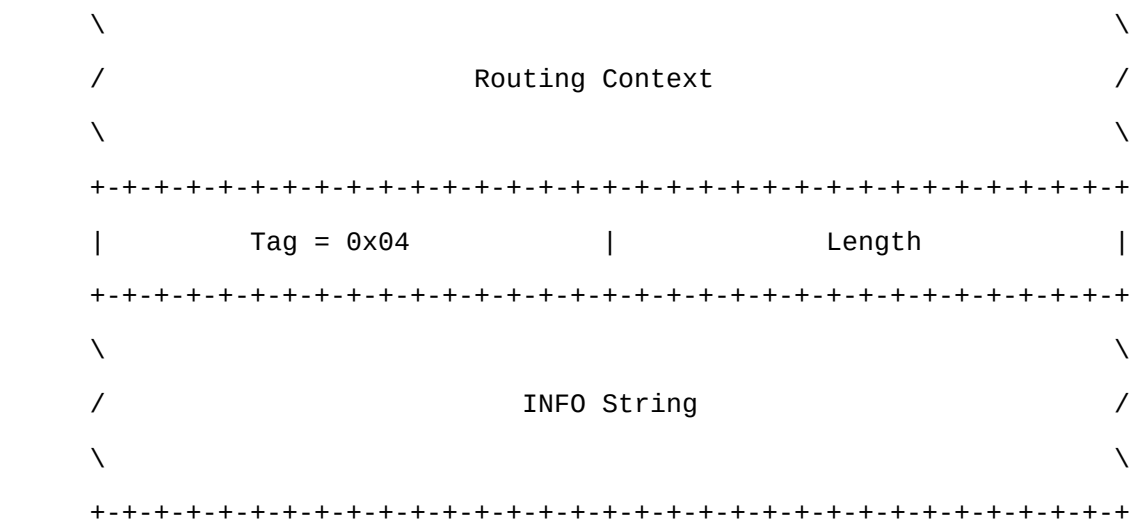
The ASP Active message contains the following parameters:

Traffic Mode Type	Mandatory
Routing Context	Optional

INFO String Optional

The format for the ASP Active message is as follows:





Traffic Mode Type: 32-bit (unsigned integer)

The Traffic Mode Type parameter identifies the traffic mode of operation of the ASP within an AS. The valid values for Traffic Mode Type are shown in the following table:

1	Over-ride
2	Load-share
3	Over-ride (Standby)
4	Load-share (Standby)

Within a particular Routing Context, Over-ride and Load-share, either active or standby, MUST NOT be mixed. The Over-ride value indicates that the ASP is operating in Over-ride mode, and the ASP takes over all traffic in an Application Server (i.e., primary/back-up operation), over-riding any currently active ASPs in the AS. In Load-share mode, the ASP will share in the traffic distribution with any other currently active ASPs. The Standby versions of the Over-ride and Load-share Types indicate that the ASP is declaring itself ready to accept traffic but leaves it up to the sender as to when the traffic is started. Over-ride (Standby) indicates that the traffic sender continues to use the currently active ASP until it can no longer send/receive traffic (i.e., the currently active ASP

transitions to state ASP-DOWN or ASP-ACTIVE). At this point the sender MUST move the standby ASP to the ASP-ACTIVE state and commence traffic. Load-share (Standby) is similar - the sender continues to load-share to the current ASPs until it is determined

that there is insufficient resources in the Load-share group. When there are insufficient ASPs, the sender MUST move the ASP to state ASP-ACTIVE.

Routing Context: n X 32-bit integers

The optional Routing Context parameter contains (a list of) integers indexing the Application Server traffic that the sending ASP is configured/registered to receive.

There is one-to-one relationship between an index entry and an SGP Routing Key or AS Name. Because an AS can only appear in one Network Appearance, the Network Appearance parameter is not required in the ASP Active message.

An Application Server Process may be configured to process traffic for more than one logical Application Server. From the perspective of an ASP, a Routing Context defines a range of signalling traffic that the ASP is currently configured to receive from the SGP. For example, an ASP could be configured to support call processing for multiple ranges of PSTN trunks and therefore receive related signalling traffic, identified by separate SS7 DPC/OPC/CIC ranges.

The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1).

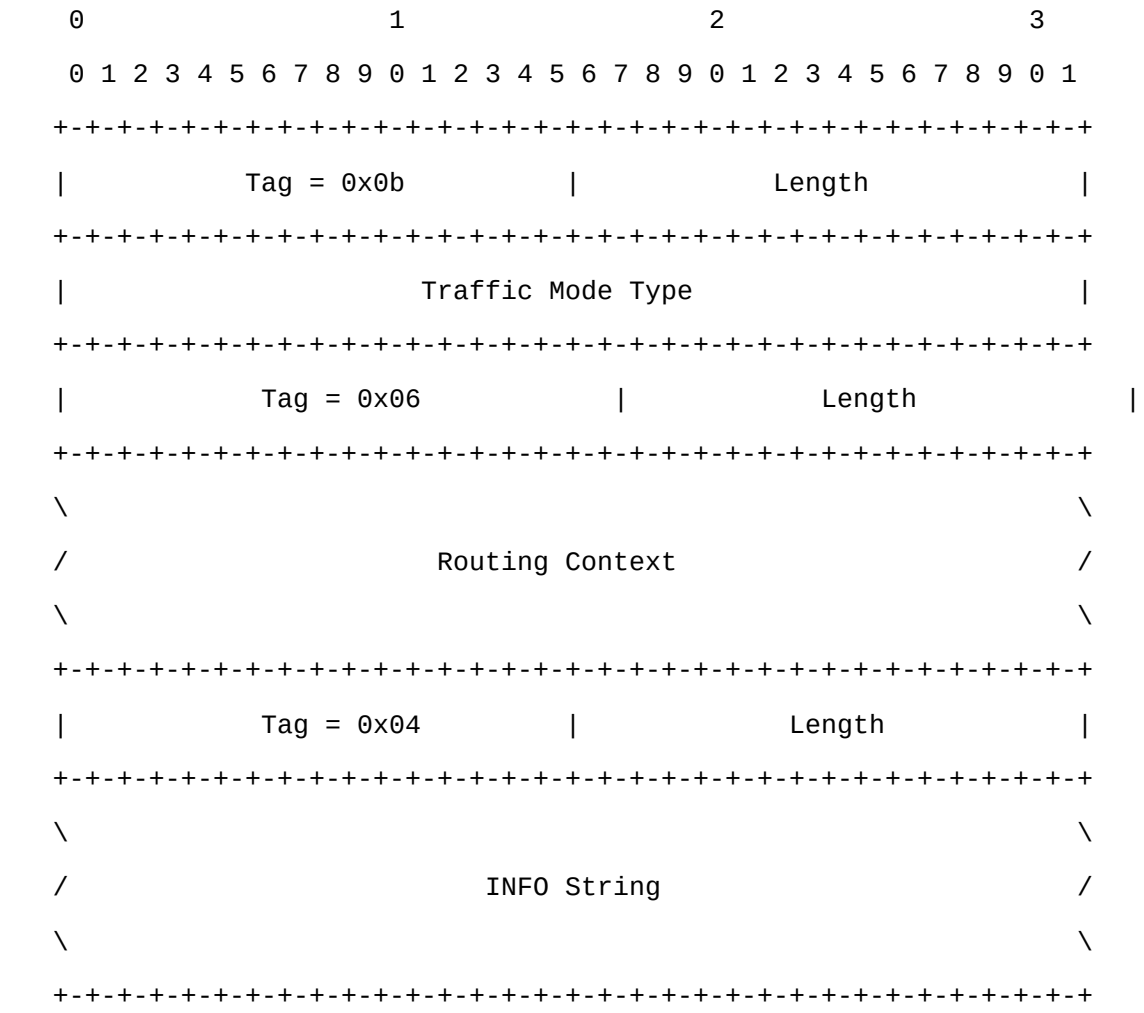
3.7.2 ASP Active Acknowledgement (ASP Active Ack)

The ASP Active Ack message is used to acknowledge an ASP Active message received from a remote M3UA peer. In the case where an ASP Active (Over-ride (standby)) or ASP Active (Load-share (standby)) message is received, a second ASP Active Ack message is sent when the ASP is moved from the ASP-STANDBY to the ASP-ACTIVE state.

The ASP Active Ack message contains the following parameters:

Traffic Mode Type	Mandatory
Routing Context	Optional
INFO String	Optional

The format for the ASP Active Ack message is as follows:



The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1).

The INFO String in an ASP Active Ack message is independent from the INFO String in the ASP Active message (i.e., it does not have to echo back the INFO String received).

The format of the Traffic Mode Type and Routing Context parameters is the same as for the ASP Active message. (See Section 3.5.5).

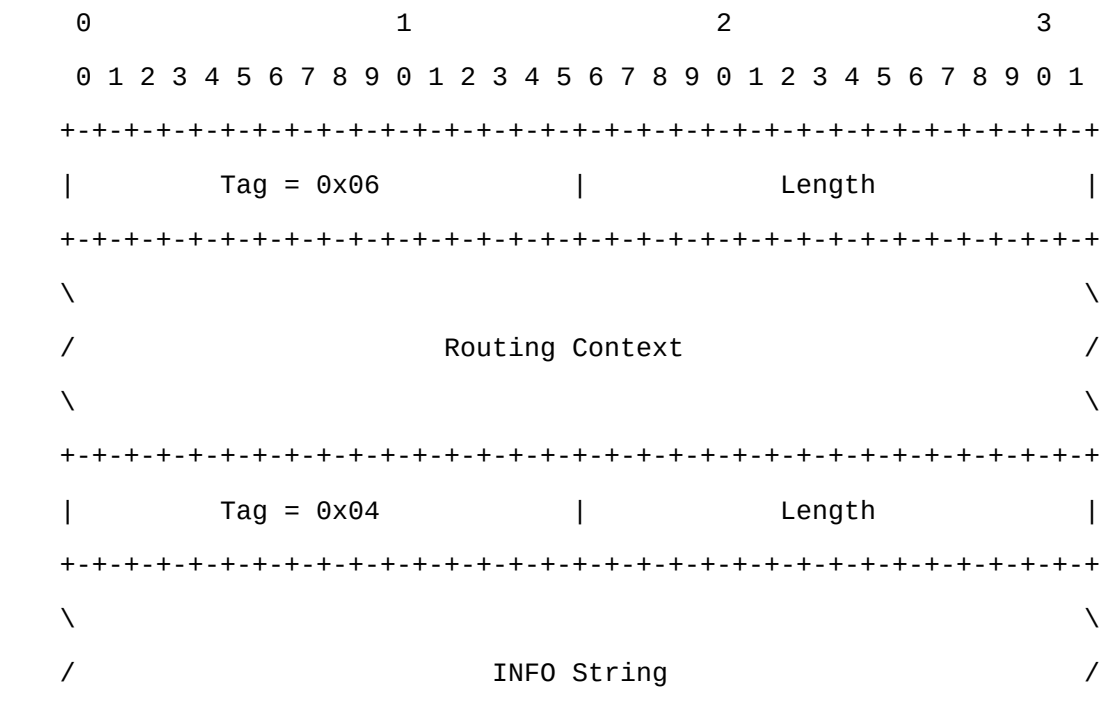
3.7.3 ASP Inactive

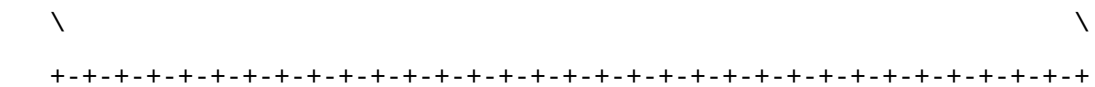
The ASP Inactive message is sent by an ASP to indicate to a remote M3UA peer
that it is no longer an active ASP to be used from within a list of ASPs. The ASP Inactive message affects only the ASP state in the Routing Keys identified by the Routing Contexts, if present.

The ASP Inactive message contains the following parameters:

Routing Context	Optional
INFO String	Optional

The format for the ASP Inactive message parameters is as follows:





The format and description of the optional Routing Context and INFO String parameters is the same as for the ASP Active message (See Section 3.5.5.)

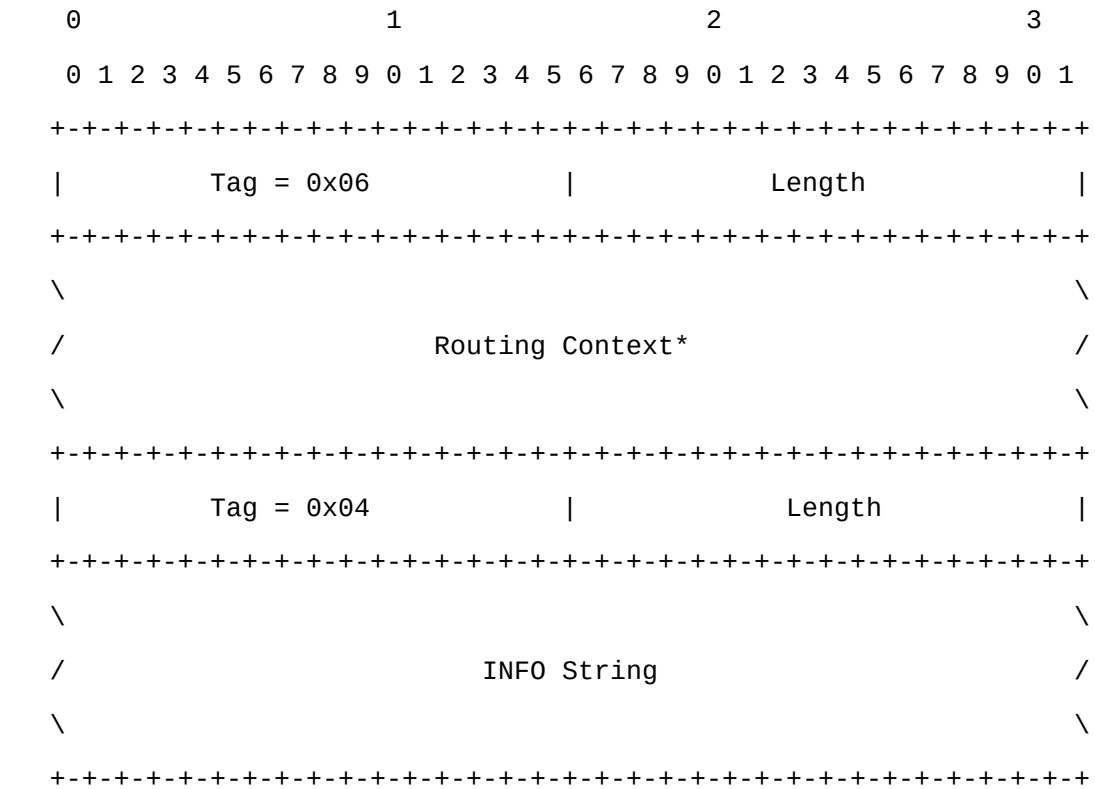
3.7.4 ASP Inactive Acknowledgement (ASP Inactive Ack)

The ASP Inactive Ack message is used to acknowledge an ASP Inactive message
received from a remote M3UA peer.

The ASP Inactive Ack message contains the following parameters:

Routing Context	Optional
INFO String	Optional

The format for the ASP Inactive Ack message is as follows:



The format and description of the optional INFO String parameter is the same as for the DUNA message (See Section 3.4.1.)

The INFO String in an ASP Inactive Ack message is independent from the INFO String in the ASP Inactive message (i.e., it does not have to echo back the INFO String received).

The format of the Routing Context parameter is the same as for the ASP Inactive message. (See Section 3.5.7).

3.8 Management (MGMT) Messages

3.8.1 Error

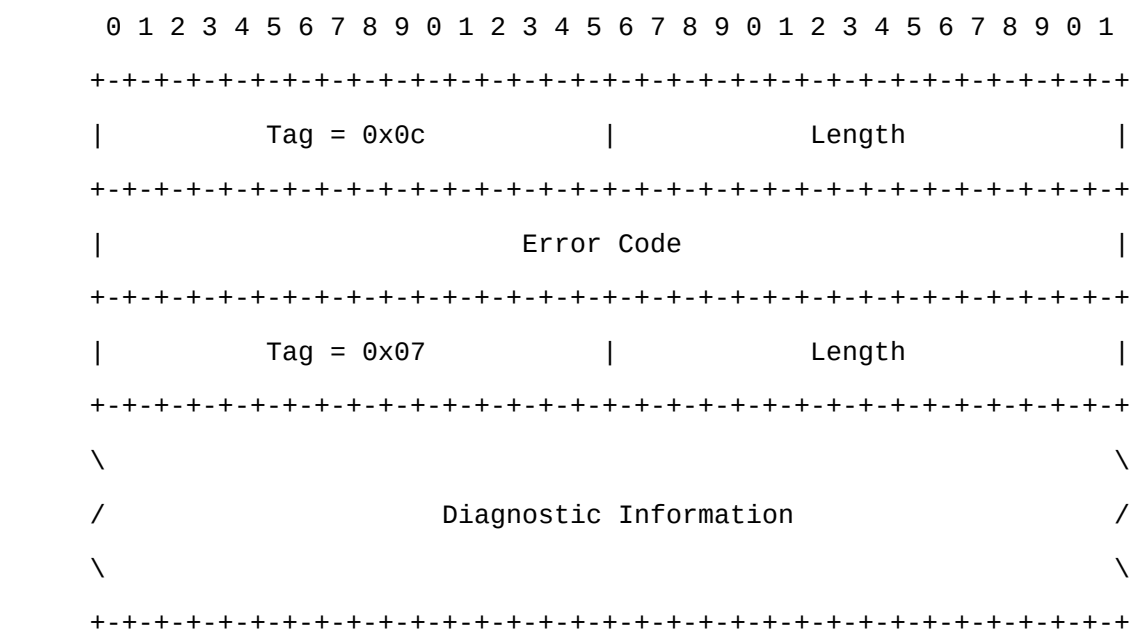
The Error message is used to notify a peer of an error event associated with an incoming message. For example, the message type might be unexpected given the current state, or a parameter value might be invalid.

The Error message contains the following parameters:

Error Code	Mandatory
Diagnostic Information	Optional

The format for the Error message is as follows:

0 1 2 3



Error Code: 32-bits (unsigned integer)

The Error Code parameter indicates the reason for the Error Message.
The Error parameter value can be one of the following values:

1	Invalid Version
2	Invalid Network Appearance
3	Unsupported Message Class

4	Unsupported Message Type
5	Unsupported/Invalid Traffic Handling Mode
6	Unexpected Message
7	Protocol Error
8	Invalid Routing Context
9	Invalid Stream Identifier

10 Invalid Parameter Value

11 Refused - Management Blocking

12 Unknown Routing Context

The "Invalid Version" error is sent if a message was received with an invalid or unsupported version. The Error message contains the supported version in the Common header. The Error message could optionally provide the supported version in the Diagnostic Information area.

The "Invalid Network Appearance" error is sent by a SGP if an ASP sends a message with an invalid (unconfigured) Network Appearance value.

The "Unsupported Message Class" error is sent if a message with an unexpected or unsupported Message Class is received.

The "Unsupported Message Type" error is sent if a message with an unexpected or unsupported Message Type is received.

The "Unsupported/Invalid Traffic Handling Mode" error is sent by a SGP if an ASP sends an ASP Active message with an unsupported Traffic Mode Type or a Traffic Mode Type that is inconsistent with the presently configured mode for the Application Server. An example would be a case in which the SGP did not support load-sharing.

The "Unexpected Message" error MAY be sent if a defined and recognized message is received that is not expected in the current state (in some cases the ASP may optionally silently discard the message and not send an Error message). For example, silent discard is used by an ASP if it received a DATA message from an SGP while it was in the ASP-INACTIVE state.

The "Protocol Error" error is sent for any protocol anomaly(i.e., reception of a parameter that is syntactically correct but unexpected in the current situation.

The "Invalid Routing Context" error is sent if a message is received from a peer with an invalid (unconfigured) Routing Context value.

The "Invalid Stream Identifier" error is sent if a message is received on an unexpected SCTP stream (e.g., a Management message was received on a stream other than "0").

The " Invalid Parameter Value " error is sent if a message is received with an invalid parameter value (e.g., a DUPU message was received with a Mask value other than "0").

The "Refused - Management Blocking" error is sent when an ASP-Up or ASP-Active message is received and the request is refused for management reasons (e.g., management lock-out").

The "Unknown Routing Context" Error is sent if a message is received from a peer without a Routing Context parameter and it is not known by configuration data which Application Servers are referenced.

Diagnostic Information: variable length

When included, the optional Diagnostic information can be any information germane to the error condition, to assist in identification of the error condition. In the case of an Invalid Network Appearance, Traffic Handling Mode, Routing Context or Parameter Value, the Diagnostic information parameter MUST be added

and include the offending parameter. In the other cases, the Diagnostic information MAY be the first 40 bytes of the offending message.

Error messages MUST NOT be generated in response to other Error messages.

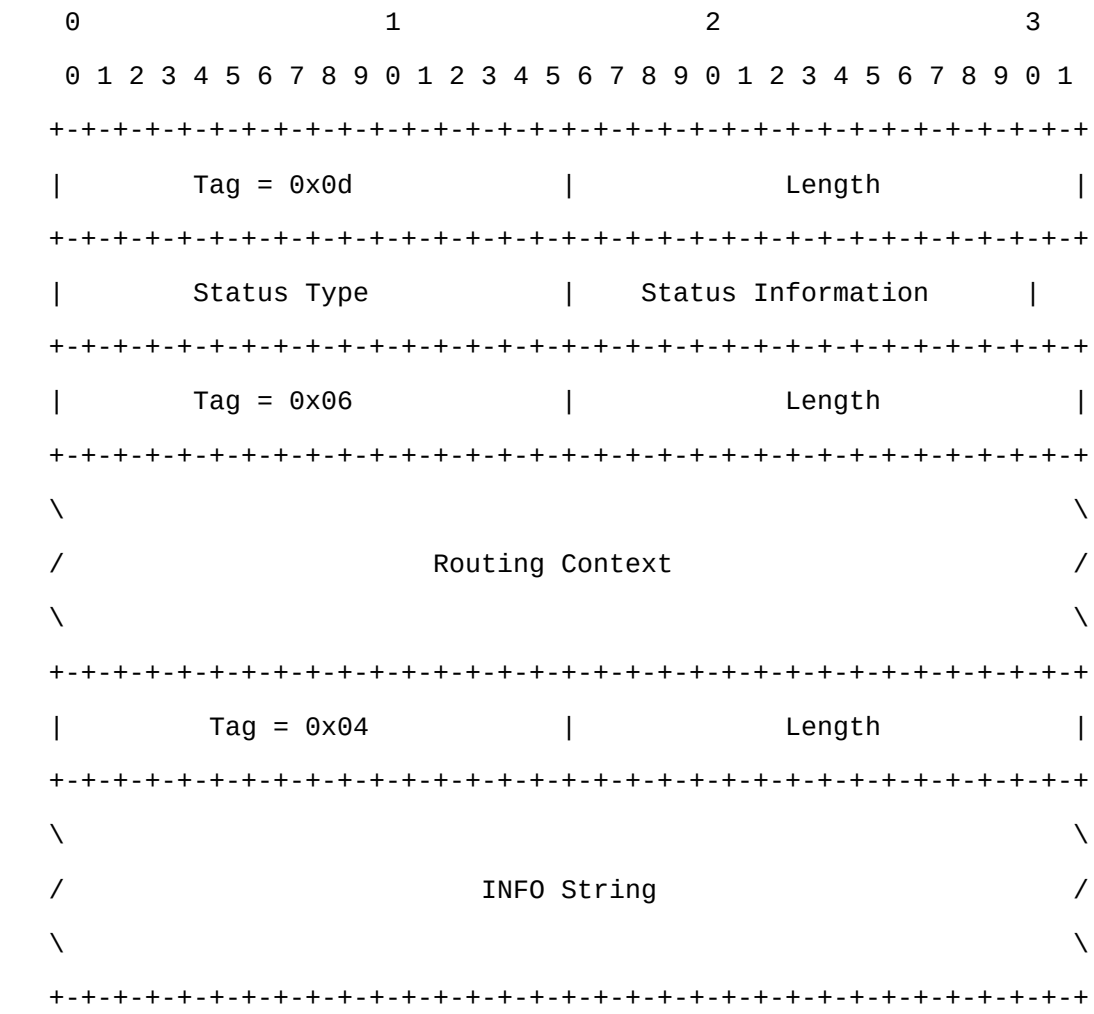
3.8.2 Notify

The Notify message used to provide an autonomous indication of M3UA events to an M3UA peer.

The Notify message contains the following parameters:

Status	Mandatory
Routing Context	Optional
INFO String	Optional

The format for the Notify message is as follows:



Status Type: 16-bits (unsigned integer)

The Status Type parameter identifies the type of the Notify message.
The following are the valid Status Type values:

1 Application Server State Change (AS-State_Change)
2 Other

Status Information: 16-bits (unsigned integer)

The Status Information parameter contains more detailed information for the notification, based on the value of the Status Type.

If the Status Type is AS-State_Change the following Status Information values are used:

1 reserved
2 Application Server Inactive (AS-INACTIVE)
3 Application Server Active (AS-ACTIVE)
4 Application Server Pending (AS-PENDING)

These notifications are sent from an SGP to an ASP upon a change in status of a particular Application Server. The value reflects the new state of the Application Server.

If the Status Type is Other, then the following Status Information values are defined:

1 Insufficient ASP Resources Active in AS
2 Alternate ASP Active

These notifications are not based on the SGP reporting the state change of an ASP or AS. In the Insufficent ASP Resources case, the SGP is indicating to an ASP_INACTIVE ASP in the AS that another ASP is required in order to handle the load of the AS (Load-sharing mode).

For the Alternate ASP Active case, an ASP is informed when an alternate ASP transitions to the ASP-ACTIVE state in Over-ride mode.

The format and description of the optional Routing Context and Info String parameters is the same as for the ASP Active message (See Section
3.5.5.)

4. Procedures

The M3UA layer needs to respond to various local primitives it receives from other layers as well as the messages that it receives from the peer M3UA layer. This section describes the M3UA procedures in response to these events.

4.1 Procedures to Support the M3UA-User and Layer Management Layers

4.1.1 Receipt of Primitives from the M3UA-User

On receiving an MTP-TRANSFER request primitive from an upper layer at an ASP/IPSP, or the nodal inter-working function at an SGP, the M3UA layer sends a corresponding DATA message (see Section 3) to its M3UA peer. The M3UA peer receiving the DATA message sends an MTP-TRANSFER indication primitive to the upper layer.

The M3UA message distribution function (see Section 1.4.2.1) determines the Application Server (AS) based on comparing the information in the MTP-TRANSFER request primitive with a provisioned Routing Key.

>From the list of ASPs within the AS table, an ASP in the ASP-ACTIVE state is selected and a DATA message is constructed and issued on the corresponding SCTP association. If more than one ASP is in the ASP-ACTIVE state (i.e., traffic is to be load-shared across more than one ASP), one of the ASPs in the ASP_ACTIVE state is selected from the

list. The selection algorithm is implementation dependent but could, for example, be round-robin or based on, for example, the SLS or ISUP CIC. The appropriate selection algorithm must be chosen carefully as it is dependent on application assumptions and understanding of the degree of state coordination between the ASP_ACTIVE ASPs in the AS.

In addition, the message needs to be sent on the appropriate SCTP stream, again taking care to meet the message sequencing needs of the signalling application.

When there is no Routing Key match, or only a partial match, for an incoming SS7 message, a default treatment MUST be specified. Possible solutions are to provide a default Application Server at the SGP that directs all unallocated traffic to a (set of) default ASP(s), or to drop the message and provide a notification to Layer Management in an M-ERROR indication primitive. The treatment of unallocated traffic is implementation dependent.

4.1.2 Receipt of Primitives from the Layer Management

On receiving primitives from the local Layer Management, the M3UA layer will take the requested action and provide an appropriate response primitive to Layer Management.

An M-SCTP_ESTABLISH request primitive from Layer Management at an ASP or IPSP will initiate the establishment of an SCTP association. The M3UA layer will attempt to establish an SCTP association with the remote M3UA peer by sending an SCTP-ASSOCIATE primitive to the local SCTP layer.

When an SCTP association has been successfully established, the SCTP will send an SCTP-COMMUNICATION_UP notification primitive to the local M3UA layer. At the SGP or IPSP that initiated the request, the M3UA layer will send an M-SCTP_ESTABLISH confirm primitive to Layer Management when the association set-up is complete. At the peer M3UA layer, an M-SCTP_ESTABLISH indication primitive is sent to Layer Management upon successful completion of an incoming SCTP association set-up.

An M-SCTP_RELEASE request primitive from Layer Management initates the tear-down of an SCTP association. The M3UA layer accomplishes a graceful shutdown of the SCTP association by sending an SCTP-SHUTDOWN primitive to the SCTP layer.

When the graceful shutdown of the SCTP association has been accomplished, the SCTP layer returns an SCTP-SHUTDOWN_COMPLETE notification primitive to the local M3UA layer. At the M3UA Layer that initiated the request, the M3UA layer will send an M-SCTP_RELEASE confirm primitive to Layer Management when the association teardown is complete. At the peer M3UA Layer, an M-SCTP_RELEASE indication primitive is sent to Layer Management upon successful tear-down of an SCTP association.

An M-SCTP_STATUS request primitive supports a Layer Management query of the local status of a particular SCTP association. The M3UA layer simply maps the M-SCTP_STATUS request primitive to an SCTP-STATUS

primitive to the SCTP layer. When the SCTP responds, the M3UA layer

maps the association status information to an M-SCTP_STATUS confirm primitive. No peer protocol is invoked.

Similar LM-to-M3UA-to-SCTP and/or SCTP-to-M3UA-to-LM primitive mappings can be described for the various other SCTP Upper Layer primitives in RFC2960 [13] such as INITIALIZE, SET PRIMARY, CHANGE HEARTBEAT, REQUEST HEARTBEAT, GET SRTT REPORT, SET FAILURE THRESHOLD, SET PROTOCOL PARAMETERS, DESTROY SCTP INSTANCE, SEND FAILURE, AND NETWORK STATUS CHANGE. Alternatively, these SCTP Upper Layer primitives (and Status as well) can be considered for modeling purposes as a Layer Management interaction directly with the SCTP Layer.

M-NOTIFY indication and M-ERROR indication primitives indicate to Layer Management the notification or error information contained in a received M3UA Notify or Error message respectively. These indications can also be generated based on local M3UA events.

An M-ASP_STATUS request primitive supports a Layer Management query of the status of a particular local or remote ASP. The M3UA layer responds with the status in an M-ASP_STATUS confirm primitive. No M3UA peer protocol is invoked.

An M-AS_STATUS request supports a Layer Management query of the status of a particular AS. The M3UA responds with an M-AS_STATUS confirm primitive. No M3UA peer protocol is invoked.

M-ASP_UP request, M-ASP_DOWN request, M-ASP_ACTIVE request and M-ASP_ INACTIVE request primitives allow Layer Management at an ASP to initiate state changes. Upon successful completion, a corresponding confirm primitive is provided by the M3UA layer to Layer Management. If an invocation is unsuccessful, an Error indication primitive is provided in the primitive.

These requests result in outgoing ASP Up, ASP Down, ASP Active and ASP Inactive messages to the remote M3UA peer at an SGP or IPSP.

4.1.3 Receipt of M3UA Peer Management Messages

Upon successful state changes resulting from reception of ASP Up, ASP Down, ASP Active and ASP Inactive messages from a peer M3UA, the M3UA layer SHOULD invoke corresponding M-ASP_UP, M-ASP_DOWN, M-ASP_ACTIVE and M-ASP_INACTIVE, M-AS_ACTIVE, M-AS_INACTIVE, and M-AS_DOWN indication primitives to the local Layer Management.

M-NOTIFY indication and M-ERROR indication primitives indicate to Layer Management the notification or error information contained in a received M3UA Notify or Error message. These indications can also be generated based on local M3UA events.

4.2 Procedures to Support the Management of SCTP Associations with M3UA Peers

These procedures support the M3UA management of SCTP Associations between SGPs and ASPs or between IPSPs.

4.2.1 AS and ASP State Maintenance

The M3UA layer on the SGP maintains the state of each remote ASP, in each Application Server that the ASP is configured to receive traffic, as input to the M3UA message distribution function. Similarly, where IPSPs use M3UA in a point-to-point fashion, the M3UA layer in an IPSP maintains the state of remote IPSPs. For the purposes of the following procedures, only the SGP/ASP case is described but the SGP side of the procedures also apply to an IPSP sending traffic to an AS consisting of

a set of remote IPSPs.

4.2.1.1 ASP States

The state of each remote ASP, in each AS that it is configured to operate, is maintained in the M3UA layer in the SGP. The state of a particular ASP in a particular AS changes due to events. The events include:

* Reception of messages from the peer M3UA layer at the ASP;
* Reception of some messages from the peer M3UA layer at other ASPs in the AS (e.g., ASP Active message indicating "Over-ride");
* Reception of indications from the SCTP layer; or
* Local Management intervention.

The ASP state transition diagram is shown in Figure 4. The possible states of an ASP are:

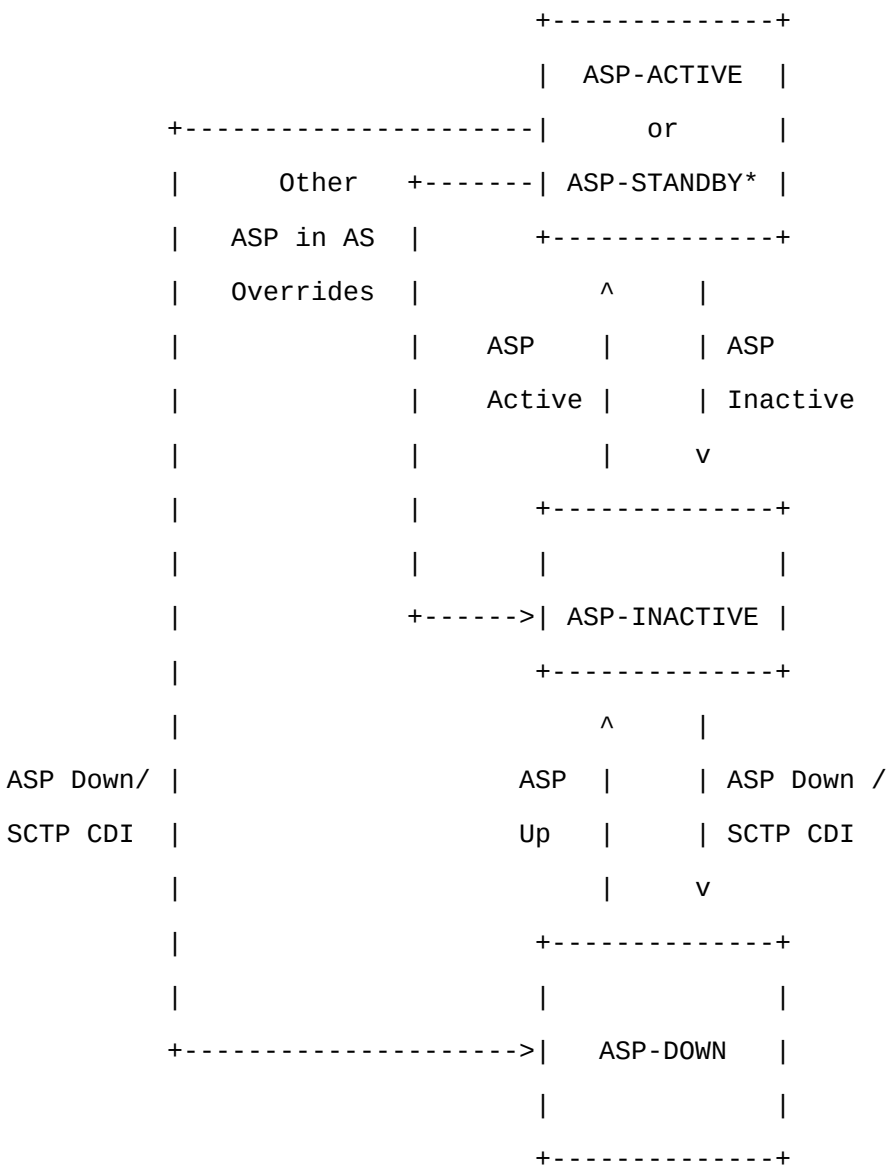
ASP-DOWN: The remote M3UA peer at the ASP is unavailable and/or the related SCTP association is down. Initially all ASPs will be in this state. An ASP in this state SHOULD NOT be sent any M3UA messages.

ASP-INACTIVE: The remote M3UA peer at the ASP is available (and the related SCTP association is up) but application traffic is stopped. In this state the ASP MAY be sent any non-DATA M3UA messages.

ASP-ACTIVE: The remote M3UA peer at the ASP is available and application traffic is active (for a particular Routing Context or set of Routing Contexts).

ASP-STANDBY: The remote M3UA peer at the ASP is available and ready to receive application traffic at any time (for a particular Routing Context or set of Routing Contexts). In this state the ASP MAY be sent any non-Data M3UA messages.

Figure 4: ASP State Transition Diagram



*Note: ASP-ACTIVE and ASP-STANDBY differ only in whether the ASP is currently receiving Data traffic within the AS.

SCTP CDI: The SCTP CDI denotes the local SCTP layer's Communication Down Indication to the Upper Layer Protocol (M3UA) on an SGP. The local SCTP layer will send this indication when it detects the loss of connectivity to the ASP's peer SCTP layer. SCTP CDI is understood as either a SHUTDOWN_COMPLETE notification or COMMUNICATION_LOST notification from the SCTP layer.

4.2.1.2 AS States

The state of the AS is maintained in the M3UA layer on the SGP. The state of an AS changes due to events. These events include:

* ASP state transitions
* Recovery timer triggers

The possible states of an AS are:

AS-DOWN: The Application Server is unavailable. This state implies that all related ASPs are in the ASP-DOWN state for this AS. Initially the AS will be in this state. An Application Server MUST be in the AS-DOWN state before it can be removed from a configuration.

AS-INACTIVE: The Application Server is available but no application traffic is active (i.e., one or more related ASPs are in the ASP-INACTIVE state, but none in the ASP-ACTIVE or ASP-STANDBY states). The recovery timer
T(r) is not running or has expired.

AS-ACTIVE: The Application Server is available and application traffic is active. This state implies that at least one ASP is in the ASP-ACTIVE state.

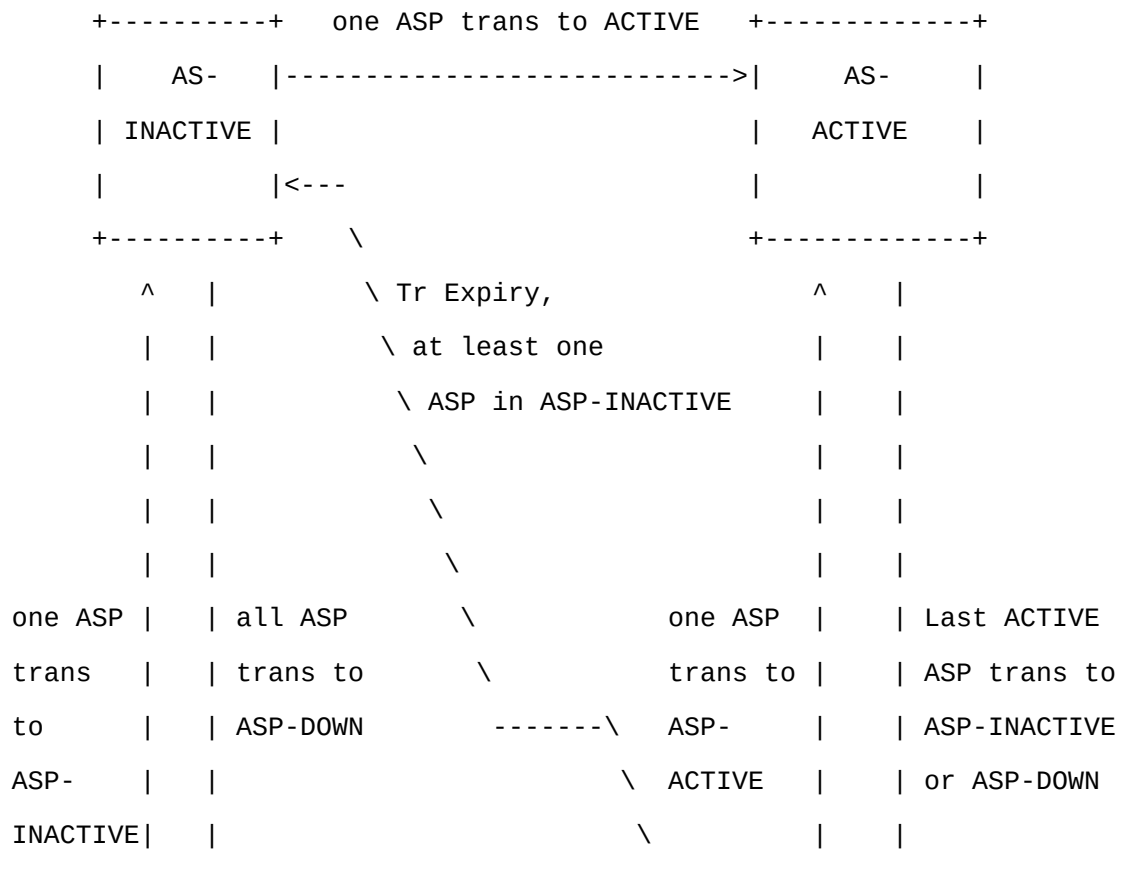
AS-PENDING: An active ASP has transitioned to ASP-INACTIVE or ASP-DOWN and it was the last remaining active ASP in the AS (and no ASPs in the ASP-STANDBY state are available. A recovery timer T(r) SHOULD be started and all incoming signalling messages SHOULD be queued by the SGP. If an ASP becomes ASP-ACTIVE before T(r) expires, the AS is moved to the AS-ACTIVE state and all the queued messages will be sent to the ASP.

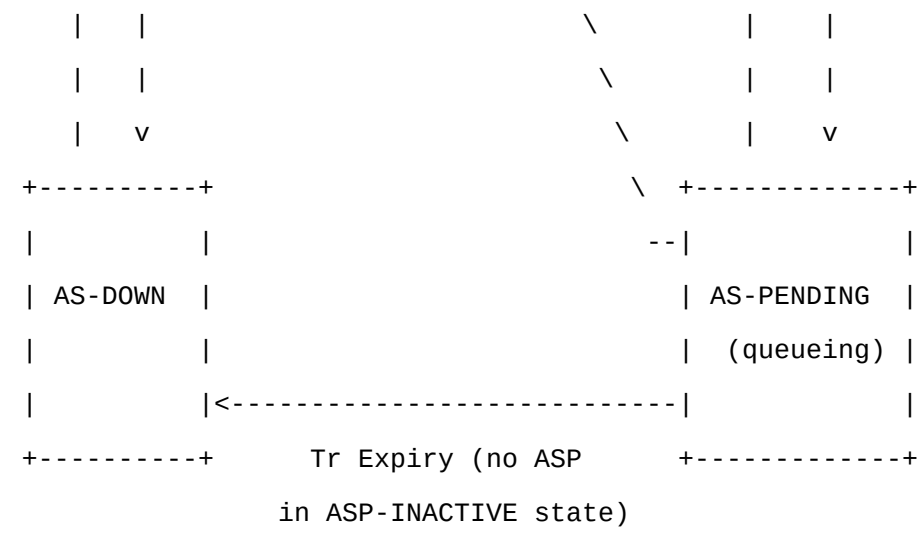
If T(r) expires before an ASP becomes ASP-ACTIVE, the SGP stops queuing messages and discards all previously queued messages. The AS will move to the AS-INACTIVE state if at least one ASP is in ASP-INACTIVE state, otherwise it will move to AS-DOWN state.

Figure 5 shows an example AS state machine for the case where the AS/ASP data is pre-configured. For other cases where the AS/ASP configuration data is created dynamically, there would be differences in the state machine, especially at creation of the AS.

For example, where the AS/ASP configuration data is not created until Registration of the first ASP, the AS-INACTIVE state is entered directly upon the first successful REG REQ from an ASP. Another example is where the AS/ASP configuration data is not created until the first ASP successfully enters the ASP-ACTIVE state. In this case the AS-ACTIVE state is entered directly.

Figure 5: AS State Transition Diagram





Tr = Recovery Timer

4.2.2 M3UA Management Procedures for Primitives

Before the establishment of an SCTP association the ASP state at both the SGP and ASP is assumed to be in the state ASP-DOWN.

Once the SCTP association is established (see Section 4.1.2) and assuming that the local M3UA-User is ready, the local M3UA ASP Maintenance (ASPM) function will initiate the relevant procedures, using the ASP Up/ASP Down/ASP Active/ASP Inactive messages to convey the ASP state to the SGP (see Section 4.3.3).

If the M3UA layer subsequently receives an SCTP-COMMUNICATION_DOWN or SCTP-RESTART indication primitive from the underlying SCTP layer, it will inform the Layer Management by invoking the M-SCTP_STATUS indication primitive. The state of the ASP will be moved to ASP-DOWN At an ASP, the MTP3-User will be informed of the unavailability of any affected SS7 destinations through the use of MTP-PAUSE indication primitives. In the case

of SS7 network isolation, the local MTP3-Users MAY be informed by implementation-dependent means, as there is currently no primitive defined for conveying this information.

In the case of SCTP-COMMUNICATION_DOWN, the SCTP client MAY try to re-establish the SCTP Association. This MAY be done by the M3UA layer automatically, or Layer Management MAY re-establish using the M-SCTP_ESTABLISH request primitive.

In the case of an SCTP-RESTART indication at an ASP, the ASP is now considered by its M3UA peer to be in the ASP-DOWN state. The ASP, if it is to recover, must begin any recovery with the ASP-Up procedure.

4.2.3 M3UA Management Procedures for Peer-to-Peer Messages

All M3UA Management and ASP State and Traffic Maintenance messages are sent on a sequenced
stream to ensure ordering. SCTP stream '0' is used.

4.2.3.1 ASP Up Procedures

After an ASP has successfully established an SCTP association to an SGP, the SGP waits for the ASP to send an ASP Up message, indicating that the ASP M3UA peer is available. The ASP is always the initiator of the ASP Up message. This action MAY be initiated at the ASP by an M-ASP_UP request primitive from Layer Management or MAY be initiated automatically by an M3UA management function.

When an ASP Up message is received at an SGP and internally the remote ASP is in the ASP-DOWN state and not considered locked-out for local management reasons, the SGP marks the remote ASP in the state ASP-

INACTIVE and informs Layer Management with an M-ASP_Up indication primitive. If the SGP is aware, via current configuration data, which Application Servers the ASP is configured to operate in, the SGP updates the ASP state to ASP-INACTIVE in each AS that it is a member. Alternatively, the SGP may move the ASP into a pool of Inactive ASPs available for future configuration within Application Server(s), determined in a subsequent Registration Request or ASP Active procedure. The SGP responds with an ASP Up Ack message in acknowledgement. The SGP sends an ASP Up Ack message in response to a received ASP Up message even if the ASP is already marked as ASP-INACTIVE at the SGP.

If for any local reason (e.g., management lock-out) the SGP cannot respond with an ASP Up Ack message, the SGP responds to an ASP Up message with an Error message with Reason "Refused - Management Blocking".

At the ASP, the ASP Up Ack message received is not acknowledged. Layer Management is informed with an M-ASP_UP confirm primitive. When an ASP

enters the ASP-Inactive state from the ASP_Down state towards an SGP the M3UA MUST mark all SS7 destinations configured to be reachable via this SGP as available.

When the ASP sends an ASP Up message it starts timer T(ack). If the ASP does not receive a response to an ASP Up message within T(ack), the ASP MAY restart T(ack) and resend ASP-Up messages until it receives an ASP Up Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Up messages MAY be put under control of Layer Management. In this method, expiry of T(ack)

results in an M-ASP_UP confirm primitive carrying a negative indication.

The ASP must wait for the ASP Up Ack message before sending any other M3UA messages (e.g., ASP Active or REG REQ). If the SGP receives any other M3UA messages before an ASP Up message is received, the SGP SHOULD discard them.

If an ASP Up message is received and internally the remote ASP is in the ASP-ACTIVE or ASP-STANDBY state, an ASP-Up Ack message is returned, as well as an Error message ("Unexpected Message), and the remote ASP state is changed to ASP-INACTIVE in all relevant Application Servers.

If an ASP Up message is received and internally the remote ASP is already in the ASP-INACTIVE state, an ASP Up Ack message is returned and no further action is taken.

4.2.3.1.1 M3UA Version Control

If an ASP Up message with an unsupported version is received, the receiving end responds with an Error message, indicating the version the receiving node supports and notifies Layer Management.

This is useful when protocol version upgrades are being performed in a network. A node upgraded to a newer version should support the older versions used on other nodes it is communicating with. Because ASPs initiate the ASP Up procedure it is assumed that the Error message would normally come from the SGP.

4.2.3.1.2 IPSP Considerations

In the case of peer-to-peer IPSPs, either of the IPSPs (IPSP_A) may start operations by sending an ASP Up message to the remote peer (IPSP_B). When the ASP Up message is received at IPSP_B and internally the remote IPSP_A is in the ASP-DOWN state and not considered locked-

out for local management reasons, IPSP_B marks the remote IPSP_A in the state ASP-INACTIVE and informs Layer Management with an M-ASP_Up indication primitive. IPSP_B returns an ASP-Up Ack message to IPSP_A. IPSP_A moves IPSP_B to the ASP-INACTIVE state upon reception of an ASP Up Ack message, if is not already in the ASP_INACTIVE state, and informs Layer Management with an M-ASP_UP confirmation primitive.

If for any local reason (e.g., management lock-out) the IPSP_B cannot respond with an ASP Up Ack message, it responds to an ASP Up message with an Error message with Reason "Refused - Management Blocking" and leaves IPSP_A in the ASP-DOWN state.

4.2.3.2 ASP-Down Procedures

The ASP will send an ASP Down message to an SGP when the ASP wishes to be
removed from service in all Application Servers that it is a member and no longer receive any DATA, SSNM or ASPTM messages. This action MAY be initiated at the ASP by an M-ASP_DOWN request primitive from Layer Management or MAY be initiated automatically by an M3UA management function.

Whether the ASP is permanently removed from any AS is a function of configuration management. In the case where the ASP previously used the Registration procedures (see Section 3.5.5) to register within Application Servers but has not deregistered from all of them prior to sending the ASP Down message, the SGP SHOULD consider the ASP as Deregistered in all Application Servers that it is still a member.

The SGP marks the ASP as ASP-DOWN, informs Layer Management with an M-ASP_Down indication primitive, and returns an ASP Down Ack message to the ASP. has locked out the ASP for management reasons.

The SGP sends an ASP Down Ack message in response to a received ASP-Down message from the ASP even if the ASP is already marked as ASP-DOWN at the SGP. The SGP sends an ASP Down Ack message even if the reason in the received ASP Down message is considered invalid.

At the ASP, the ASP Down Ack message received is not acknowledged. Layer Management is informed with an M-ASP_DOWN confirm primitive. If the ASP receives an ASP Down Ack without having sent an ASP Down message, the ASP should now consider itself as in the ASP-DOWN state. If the ASP was previously in the ASP-ACTIVE or ASP_INACTIVE state, the ASP should then initiate procedures to return itself to its previous state.

When the ASP sends an ASP Down message it starts timer T(ack). If the ASP does not receive a response to an ASP Down message within T(ack), the ASP MAY restart T(ack) and resend ASP Down messages until it receives an ASP Down Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Down messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in an M-ASP_DOWN confirm primitive carrying a negative indication.

4.2.3.4 ASP-Active Procedures

Anytime after the ASP has received an ASP Up Ack message from the SGP or IPSP, the ASP sends an ASP Active message to the SGP indicating that the ASP is ready to start processing traffic. This action MAY be initiated at the ASP by an M-ASP_ACTIVE request primitive from Layer Management or MAY be initiated automatically by an M3UA management function. In the case where an ASP wishes to process the traffic for more than one Application Server across a common SCTP association, the ASP Active message(s) SHOULD contain a list of one or more Routing Contexts to indicate for which Application Servers the ASP Active message applies. It is not necessary for the ASP to include all Routing Contexts of interest in a single ASP Active message, thus requesting to become active in all Routing Contexts at the same time. Multiple ASP Active messages MAY be used to activate within the Application Servers independently, or in sets. In the case where an ASP Active message does not contain a Routing Context parameter, the receiver must know, via configuration data, which Application Server(s) the ASP is a member.

For the Application Servers that the ASP can be successfully activated, he SGP or IPSP responds
with one or more ASP Active Ack messages, including the associated Routing Context and Traffic Mode Type values. The Routing Context parameter MUST be included in the Asp Active Ack message if the received ASP Active message contained any Routing Contexts. Depending on the ASP Active Message Traffic Mode Type request, the SGP moves the ASP to the correct ASP traffic state within the associated Application Server(s). Layer Management is informed with an M-ASP_Active indication. If the SGP or IPSP receives any Data messages before an ASP Active message is received, the SGP or IPSP MAY discard them. By sending an ASP Active Ack message, the SGP or IPSP is now ready to receive and send traffic for the related Routing Context(s). The ASP SHOULD NOT send Data messages for the related Routing Context(s) before receiving an ASP Active Ack message, or it will risk message loss.

Multiple ASP Active Ack messages MAY be used in response to an ASP Active message containing multiple Routing Contexts, allowing the SGP or IPSP to independently acknowledge the ASP Active message for different (sets of) Routing Contexts. The SGP or IPSP sends an Error message ("Invalid Routing Context") for each Routing Context value that the ASP cannot be successfully activated .

In the case where an "out-of-the-blue" ASP Active message is received (i.e., the ASP has not registered with the SG or the SG has no static configuration data for the ASP), the message may be silently discarded.

The SGP MUST send an ASP Active Ack message in response to a received ASP Active message from the ASP, if the ASP is already marked in the ASP-ACTIVE state at the SGP.

At the ASP, the ASP Active Ack message received is not acknowledged. Layer Management is informed with an M-ASP_ACTIVE confirm primitive. It is possible for the ASP to receive Data message(s) before the ASP Active Ack message as the ASP Active Ack and Data messages from an SG or IPSP may be sent on different SCTP streams. Message loss is possible as the ASP does not consider itself in the ASP-ACTIVE state until reception of the ASP Active Ack message.

When the ASP sends an ASP Active message it starts timer T(ack). If the ASP does not receive a response to an ASP Active message within T(ack), the ASP MAY restart T(ack) and resend ASP Active messages until it receives an ASP Active Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Active

messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in an M-ASP_ACTIVE confirm primitive carrying a negative indication.

There are four modes of Application Server traffic handling in the SGP M3UA layer - Over-ride, Over-ride (Standby), Load-share and Load-share (Standby). The Traffic Mode Type parameter in the ASP Active message indicates the traffic handling mode used in a particular Application Server. If the SGP determines that the mode indicated in an ASP Active message is unsupported or incompatible with the mode currently configured for the AS, the SGP responds with an Error message ("Unsupported / Invalid Traffic Handling Mode"). If the Traffic Handling mode of the Application Server is not already known via configuration data, then the Traffic Handling mode indicated in the first ASP Active message causing the transition of the Application Server state to AS-ACTIVE MAY be used to set the mode.

In the case of an Over-ride mode AS, reception of an ASP Active message at an SGP causes the (re)direction of all traffic for the AS to the ASP that sent the ASP Active message. Any previously active ASP in the AS is now considered to be in state ASP-INACTIVE and SHOULD no longer receive traffic from the SGP within the AS. The SGP or IPSP then MUST send a Notify message ("Alternate ASP-Active") to the previously active ASP in the AS, and SHOULD stop traffic to/from that ASP. The ASP receiving this Notify MUST consider itself now in the ASP-INACTIVE state, if it is not already aware of this via inter-ASP communication with the Over-riding ASP.

In the case of Over-ride (Standby) mode the traffic is not started to the ASP until the currently active ASP transitions to the ASP-INACTIVE or ASP-DOWN state. At this point the ASP that sent the ASP Active message ("Over-Ride (Standby)") is moved to the ASP-ACTIVE state and the traffic is redirected. A second ASP Active Ack message with a new Traffic Mode Type ("Over-ride", previously "Over-ride(Standby)") is sent to the ASP. A Notify message ("Alternate ASP-Active") is not sent

in this case.

If there is no currently active ASP, an ASP Active Ack message ("Over-ride") is returned right away and the traffic is directed to the ASP.

In the case of a Load-share mode AS, reception of an ASP Active message at an SGP or IPSP causes the direction of traffic to the ASP sending the ASP Active message, in addition to all the other ASPs that are currently active in the AS. The algorithm at the SGP for load-sharing traffic within an AS to all the active ASPs is implementation dependent. The algorithm could, for example, be round-robin or based on information in the Data message (e.g., the SLS, SCCP SSN, ISUP CIC value).

An SGP or IPSP, upon reception of an ASP Active message for the first ASP in a Loadshare AS, MAY choose not to direct traffic to a newly active ASP until it determines that there are sufficient resources to handle the expected load (e.g., until there are "n" ASPs in state ASP-ACTIVE in the AS).

In the case of a Load-share (Standby) mode AS, the traffic is not started to the ASP until the SGP or IPSP determines that there are insufficient resources available in the AS. This is likely when one of the active load-sharing ASPs transitions to either the ASP-INACTIVE or ASP-DOWN state. At this point the ASP that sent the ASP Active message ("Load-share (Standby)") is moved to the ASP_ACTIVE state and traffic is started. A second ASP Active Ack message with a new Traffic Mode Type ("Load-share" - previously "Loadshare(Standby)") is sent to the

ASP. A Notify message ("Insufficient ASP resources active in AS ") is not sent in this case.

If there is no currently active ASP, an ASP Active Ack message ("Loadshare") is returned right away and the traffic is directed to the ASP.

All ASPs within a load-sharing mode AS must be able to process any Data message received for the AS, in order to accommodate any potential fail-over or rebalancing of the offered load.

4.2.3.5 ASP Inactive Procedures

When an ASP wishes to withdraw from receiving traffic within an AS, the ASP sends an ASP Inactive message to the SGP or IPSP. This action MAY be initiated at the ASP by an M-ASP_INACTIVE request primitive from Layer Management or MAY be initiated automatically by an M3UA management function. In the case where an ASP is processing the traffic for more than one Application Server across a common SCTP association, the ASP Inactive message contains one or more Routing Contexts to indicate for which Application Servers the ASP Inactive message applies. In the case where an ASP Inactive message does not contain a Routing Context parameter, the receiver must know, via

configuration data, which Application Servers the ASP is a member and move the ASP to the ASP-INACTIVE state in each all Application Servers. In the case of an Over-ride mode AS, where another ASP has already taken over the traffic within the AS with an ASP Active ("Over-ride") message, the ASP that sends the ASP Inactive message is already

considered by the SGP to be in state ASP-INACTIVE. .An ASP Inactive Ack message is sent to the ASP, after ensuring that all traffic is stopped to the ASP.

In the case of a Load-share mode AS, the SGP moves the ASP to the ASP-INACTIVE state and the AS traffic is re-allocated across the remaining ASPs in the state ASP-ACTIVE, as per the load-sharing algorithm currently used within the AS. A Notify message("Insufficient ASP resources active in AS") MAY be sent to all inactive ASPs, if required. However, if a Loadshare ("Standby") ASP is available, it may be now immediately included in the loadshare group and a Notify message is not sent. An ASP Inactive Ack message is sent to the ASP after all traffic is halted and Layer Management is informed with an M-ASP_INACTIVE indication primitive.

Multiple ASP Inactive Ack messages MAY be used in response to an ASP Inactive message containing multiple Routing Contexts, allowing the SGP or IPSP to independently acknowledge for different (sets of) Routing Contexts. The SGP or IPSP sends an Error message ("Invalid Routing Context") message for each invalid or un-configured Routing Context value in a received ASP Inactive message message.

The SGP MUST send an ASP Inactive Ack message in response to a received ASP Inactive message from the ASP and the ASP is already marked as ASP-INACTIVE at the SGP.

At the ASP, the ASP-Inactive Ack message received is not acknowledged. Layer Management is informed with an M-ASP_INACTIVE confirm primitive. When the ASP sends an ASP Inactive message it starts timer T(ack). If the ASP does not receive a response to an ASP Inactive message within T(ack), the ASP MAY restart T(ack) and resend ASP Inactive messages until it receives an ASP Inactive Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Inactive messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in a M-

ASP_Inactive confirm primitive carrying a negative indication.

If no other ASPs in the Application Server are in the state ASP-ACTIVE or ASP-STANDBY, the SGP MUST send a Notify message ("AS-Pending") to all of the ASPs in the AS which are in the state ASP-INACTIVE. The SGP SHOULD start buffering the incoming messages for T(r)seconds, after which messages MAY be discarded. T(r) is configurable by the network operator. If the SGP receives an ASP Active message from an ASP in the AS before expiry of T(r), the buffered traffic is directed to that ASP and the timer is cancelled. If T(r) expires, the AS is moved to the AS-INACTIVE state.

4.2.3.6 Notify Procedures

A Notify message reflecting a change in the AS state SHOULD be sent to all ASPs in the AS, except those in the ASP-DOWN state, with appropriate Status Information. The Notify message MUST be sent after any ASP State or Traffic Management acknowledgement messages (e.g., ASP Up Ack, ASP Down Ack, ASP Active Ack, or ASP Inactive Ack). At the ASP, Layer Management is informed with an M-NOTIFY indication primitive.

In the case where a Notify message("AS-Pending") message is sent by an SGP that now has no ASPs active to service the traffic, or where a Notify message("Insufficient ASP resources active in AS") is sent in the Loadshare mode, the Notify message does not explicitly compel the ASP(s) receiving the message to become active. The ASPs remain in control of what (and when) traffic action is taken.

In the case where a Notify message does not contain a Routing Context parameter, the receiver must know, via configuration data, of which Application Servers the ASP is a member and take the appropriate action for the ASP in each AS.

4.2.3.7 Heartbeat Procedures

The optional Heartbeat procedures MAY be used when operating over transport layers that do not have their own heartbeat mechanism for detecting loss of the transport association (i.e., other than SCTP).

After receiving an ASP Up Ack message from an M3UA peer in response to an ASP Up message, an ASP may optionally send Heartbeat messages periodically, subject to a provisionable timer T(beat). Upon receiving a Heartbeat message, the M3UA peer MUST respond with a Heartbeat ACK message.

At the ASP, if no Heartbeat Ack message (or any other M3UA message) is received from the M3UA peer within 2*T(beat), the remote M3UA peer is considered unavailable. Transmission of Heartbeat messages is stopped and the ASP SHOULD attempt to re-establish communication with the SGP M3UA peer.

The Heartbeat message may optionally contain an opaque Heartbeat Data parameter that MUST be echoed back unchanged in the related Heartbeat Ack message. The ASP, upon examining the contents of the returned Heartbeat Ack message, MAY choose to consider the remote M3UA peer as unavailable. The contents/format of the Heartbeat Data parameter is implementation-dependent and only of local interest to the original sender. The contents may be used, for example, to support a Heartbeat sequence algorithm (to detect missing Heartbeats), and/or a timestamp mechanism (to evaluate delays).

Note: Heartbeat related events are not shown in Figure 4 "ASP state transition diagram".

4.2.4 Routing Key Management Procedures

4.2.4.1 Registration

An ASP MAY dynamically register with an SGP as an ASP within an Application Server using the REG REQ message. A Routing Key parameter in the REG REQ message specifies the parameters associated with the Routing Key.

The SGP examines the contents of the received Routing Key parameter and compares it with the currently provisioned Routing Keys. If the received Routing Key matches an existing SGP Routing Key entry, and the ASP is not currently included in the list of ASPs for the related Application Server, the SGP MAY authorize the ASP to be added to the AS. Or, if the Routing Key does not currently exist and the received Routing Key data is valid and unique, an SGP supporting dynamic configuration MAY authorize the creation of a new Routing Key and related Application Server and add the ASP to the new AS. In either case, the SGP returns a Registration Response message to the ASP, containing the same Local-RK-Identifier as provided in the initial request, and a Registration Result "Successfully Registered". A unique Routing Context value assigned to the SGP Routing Key is included. The method of Routing Context value assignment at the SG/SGP is implementation dependent but must be guaranteed to be unique across all SGPs in an SG.

If the SGP determines that the received Routing Key data is invalid, or

contains invalid parameter values, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Invalid Routing Key", "Error - Invalid DPC", "Error - Invalid Network Appearance" as appropriate.

If the SGP determines that a unique Routing Key cannot be created, the SGP returns a Registration Response message to the ASP, with a Registration Status of "Error - "Cannot Support Unique Routing" An incoming signalling message received at an SGP should not match against more than one Routing Key.

If the SGP does not authorize the registration request, the SGP returns a REG RSP message to the ASP containing the Registration Result "Error û Permission Denied".

If an SGP determines that a received Routing Key does not currently exist and the SGP does not support dynamic configuration, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Routing Key not Currently Provisioned".

If an SGP determines that a received Routing Key does not currently exist and the SGP supports dynamic configuration but does not have the capacity to add new Routing Key and Application Server entries, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Insufficient Resources".

If an SGP determines that one or more of the Routing Key parameters are not supported for the purpose of creating new Routing Key entries, the

SGP returns a Registration Response message to the ASP, containing a Registration Result "Error û Unsupported RK parameter field". This result MAY be used if, for example, the SGP does not support RK Circuit Range Lists in a Routing Key because the SGP does not support ISUP traffic, or does not provide CIC range granularity.

A Registration Response "Error û Unsupported Traffic Handling Mode" is returned if the Routing Key in the REG REQ contains an Traffic Handling Mode that is inconsistent with the presently configured mode for the matching Application Server.
An ASP MAY register multiple Routing Keys at once by including a number of Routing Key parameters in a single REG REQ message. The SGP MAY respond to each registration request in a single REG RSP message, indicating the success or failure result for each Routing Key in a separate Registration Result parameter. Alternatively the SGP MAY respond with multiple REG RSP messages, each with one or more Registration Result parameters. The ASP uses the Local-RK-Identifier parameter to correlate the requests with the responses.

Upon successful registration of an ASP in an AS, the SGP can now send related SS7 Signalling Network Management messaging, if this did not previously start upon the ASP transitioning to state ASP-INACTIVE

4.2.4.2 Deregistration

An ASP MAY dynamically deregister with an SGP as an ASP within an Application Server using the DEREG REQ message. A Routing Context parameter in the DEREG REQ message specifies which Routing Keys to de-register. An ASP SHOULD move to the ASP-INACTIVE state for an Application Server before attempting to deregister the Routing Key (i.e., deregister after receiving an ASP Inactive Ack). Also, an ASP SHOULD deregister from all Application Servers that it is a member before attempting to move to the ASP-Down state.

The SGP examines the contents of the received Routing Context parameter and validates that the ASP is currently registered in the Application Server(s) related to the included Routing Context(s). If validated, the ASP is de-registered as an ASP in the related Application Server.

The deregistration procedure does not necessarily imply the deletion of Routing Key and Application Server configuration data at the SGP. Other ASPs may continue to be associated with the Application Server, in which case the Routing Key data MUST NOT be deleted. If a Deregistration results in no more ASPs in an Application Server, an SGP MAY delete the Routing Key data.

The SGP acknowledges the deregistration request by returning a DEREG RSP message to the requesting ASP. The result of the deregistration is found in the Deregistration Result parameter, indicating success or failure with cause.

An ASP MAY deregister multiple Routing Contexts at once by including a number of Routing Contexts in a single DEREG REQ message. The SGP MAY respond to each deregistration request in a single DEREG RSP message, indicating the success or failure result for each Routing Context in a separate Deregistration Result parameter.

4.3 Procedures to Support the Availability or Congestion Status of SS7 Destination

4.3.1 At an SGP

On receiving an MTP-PAUSE, MTP-RESUME or MTP-STATUS indication primitive from the nodal inter-working function at an SGP, the SGP M3UA layer will send a corresponding SS7 Signalling Network Management (SSNM) DUNA, DAVA, SCON, or DUPU message (see Section 3.4) to the M3UA peers at concerned ASPs. The M3UA layer must fill in various fields of the SSNM messages consistently with the information received in the primitives.

The SGP M3UA layer determines the set of concerned ASPs to be informed based on the SS7 network partition for which the primitive indication is relevant. In this way, all ASPs configured to send/receive traffic within a particular network appearance are informed. If the SGP operates within a single SS7 network appearance, then all ASPs are informed.

The SG M3UA MAY filter further based on the Affected Point Code in the MTP-PAUSE, MTP-RESUME or MTP-STATUS indication primitives. In this way ASPs can be informed only of affected destinations to which they actually communicate. The SGP M3UA layer MAY also suppress DUPU messages to ASPs that do not implement an MTP3-User protocol peer for the affected MTP3-User.

DUNA, DAVA, SCON, and DRST messages MUST be sent sequentially and processed at the receiver in the order sent. SCTP stream "0" is used to provide the sequencing. . The only exception to this is if the international congestion method (see Q.704) is used. If so, the Unordered bit in the SCTP DATA chunk MAY be used for the SCON message.

Sequencing is not required for the DUPU or DAUD messages, which MAY be sent un-sequenced. Again, SCTP stream 0 is used, with optional use of the Unordered bit in the SCTP DATA chunk.

4.3.2 At an ASP

4.3.2.1 Single SGP Configurations

At an ASP, upon receiving an SS7 Signalling Network Management (SSNM) message from the remote M3UA Peer, the M3UA layer invokes the appropriate primitive indications to the resident M3UA-Users. Local management is informed.

In the case where a local event has caused the unavailability or congestion status of SS7 destinations, the M3UA layer at the ASP MUST pass up appropriate indications in the primitives to the M3UA User, as though equivalent SSNM messages were received. For example, the loss of an SCTP association to an SGP may cause the unavailability of a set of SS7 destinations. MTP-PAUSE indication primitives to the M3UA User are appropriate. To accomplish this, the M3UA layer at an ASP maintains the status of routes via the SG(P), much like an MTP3 layer maintains route-set status.

4.3.2.2 Multiple SGP Configurations

At an ASP, upon receiving a Signalling Network Management message from the remote M3UA Peer, the M3UA layer updates the status of the affected route(s) via the originating SGP and determines, whether or not the overall availability or congestion status of the effected destination(s) has changed. If so, the M3UA layer invokes the appropriate primitive indications to the resident M3UA-Users. Local management is informed.

An M3UA layer at the ASP MAY choose to maintain knowledge of which SGPs

are included in Signalling Gateways for the purpose of interpreting SSNM messaging from one SGP so as to apply to all the SGPs in the SG.

4.3.3 ASP Auditing

An ASP may optionally initiate an audit procedure in order to enquire of an SGP the availability and, if the national congestion method with multiple congestion levels and message priorities is used, congestion status of an SS7 destination or set of destinations. A Destination Audit (DAUD) message is sent from the ASP to the SGP requesting the current availability and congestion status of one or more SS7 Destination Point Codes.

The DAUD message MAY be sent un-sequenced. The DAUD MAY be sent by the ASP in the following cases:

- Periodic. A Timer originally set upon reception of a DUNA, SCON or DRST message has expired without a subsequent DAVA, DUNA, SCON or DRST message updating the availability/congestion status of the affected Destination Point Codes. The Timer is reset upon issuing a DAUD. In this case the DAUD is sent to the SGP that originally sent the SSNM message.

- Isolation. The ASP is newly ASP-INACTIVE or ASP-ACTIVE or has been isolated from an SGP for an extended period. The ASP MAY request the availability/congestion status of one

or more SS7 destinations to which it expects to communicate.

In the first of the cases above, the auditing procedure must not be invoked for the case of a received SCON message containing a congestion level value of "no congestion" or undefined" (i.e., congestion Level = "0"). This is because the value indicates either congestion abatement or that the ITU MTP3 international congestion method is being used. In the international congestion method, the MTP3 layer at the SGP does not maintain the congestion status of any destinations and therefore the SGP cannot provide any congestion information in response to the DAUD. For the same reason, in the second of the cases above a DAUD message cannot reveal any congested destination(s).

The SGP MUST respond to a DAUD message with the MTP3 availability/congested status of the routeset associated with each Destination Point Code(s) in the DAUD message. The status of each SS7 destination requested is indicated in a DUNA message (if unavailable), a DAVA message (if available), or a DRST (if restricted and the SGP supports this feature). If the SS7 destination is available and congested, the SGP responds with an SCON message in addition to the DAVA message. If the SS7 destination is restricted and congested, the SGP responds with an SCON message in addition to the DRST. If the SGP has no information on the availability/congestion status of the SS7 destination, the SGP responds with a DUNA message, as it has no routing information to allow it to route traffic to this destination

Any DUNA or DAVA message in response to a DAUD message MAY contain a list of up to sixteen Affected Point Codes.

4.4 MTP3 Restart

In the case where the MTP3 in the SG undergoes an MTP restart, event communication SHOULD be handled as follows:

When the SG discovers SS7 network isolation, the SGPs send an indication to all concerned available ASPs (i.e., ASPs in the ASP-ACTIVE, ASP-STANDBY or ASP-INACTIVE state) using a DUNA message. For the purpose of MTP restart, all Signalling Point Management Clusters with point codes

different from that of the SG with at least one ASP in the ASP-ACTIVE state or that has sent an ASP ACTIVE message to the SG during the first part of the restart procedure should be considered as available. If the M3UA layer at the SGP receives any ASP ACTIVE messages during the restart procedure, it delays the ASP ACTIVE ACK messages until the end of the restart procedure. During the second part of the restart procedure the SGP M3UA layers at the SGPs inform all concerned ASPs in the ASP-ACTIVE, ASP-STANDBY or ASP-INACTIVE states of any unavailable SS7 destinations using the DUNA message. At the end of the restart procedure the SGP M3UA layers send an ASP ACTIVE ACK message to all ASPs in the ASP-ACTIVE state.

When the M3UA layer at an ASP receives a DUNA message indicating SS7 network isolation at an SG, it will stop any affected traffic via this route. When the M3UA subsequently receives any DUNA messages from an SGP it will mark the affected SS7 destinations as unavailable via that SG. When the M3UA receives an ASP ACTIVE ACK message it can resume traffic to available SS7 destinations via this SGP, provided the ASP is in the ASP-ACTIVE state towards this SGP. The ASP MAY choose to audit the availability of any unavailable destinations

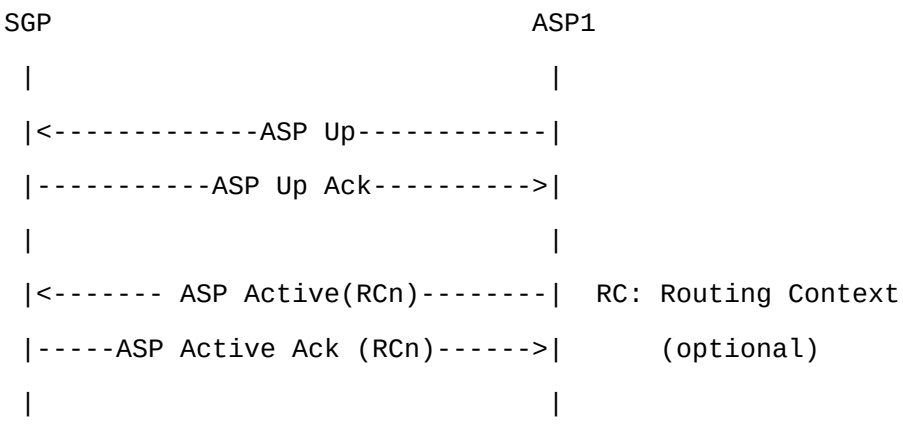
5. Examples of M3UA Procedures

5.1 Establishment of Association and Traffic between SGPs and ASPs

5.1.1 Single ASP in an Application Server ("1+0" sparing),

5.1.1.1 Single ASP in an Application Server ("1+0" sparing), No Registration

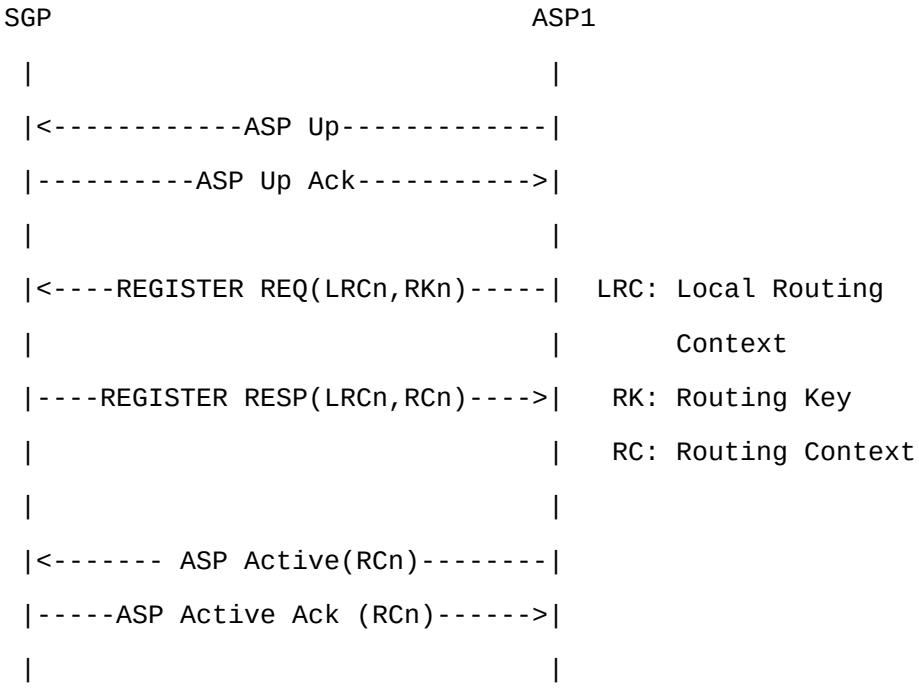
This scenario shows the example M3UA message flows for the establishment of traffic between an SGP and an ASP, where only one ASP is configured within an AS (no backup). It is assumed that the SCTP association is already set-up. The sending of any DUNA/SCON messages by the SGP is not shown but is similar to the case described in Section 5.1.2.



Note: If the ASP Active message contains an optional Routing Context parameter, The ASP Active message only applies for the specified RC value(s). For an unknown RC value, the SGP responds with an Error message.

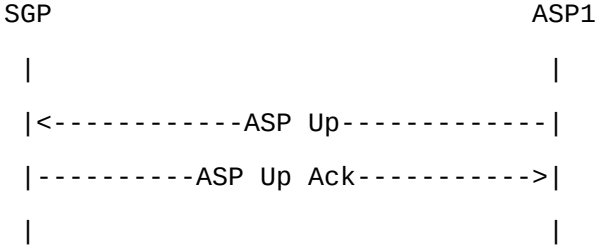
5.1.1.2 Single ASP in Application Server ("1+0" sparing), Dynamic Registration

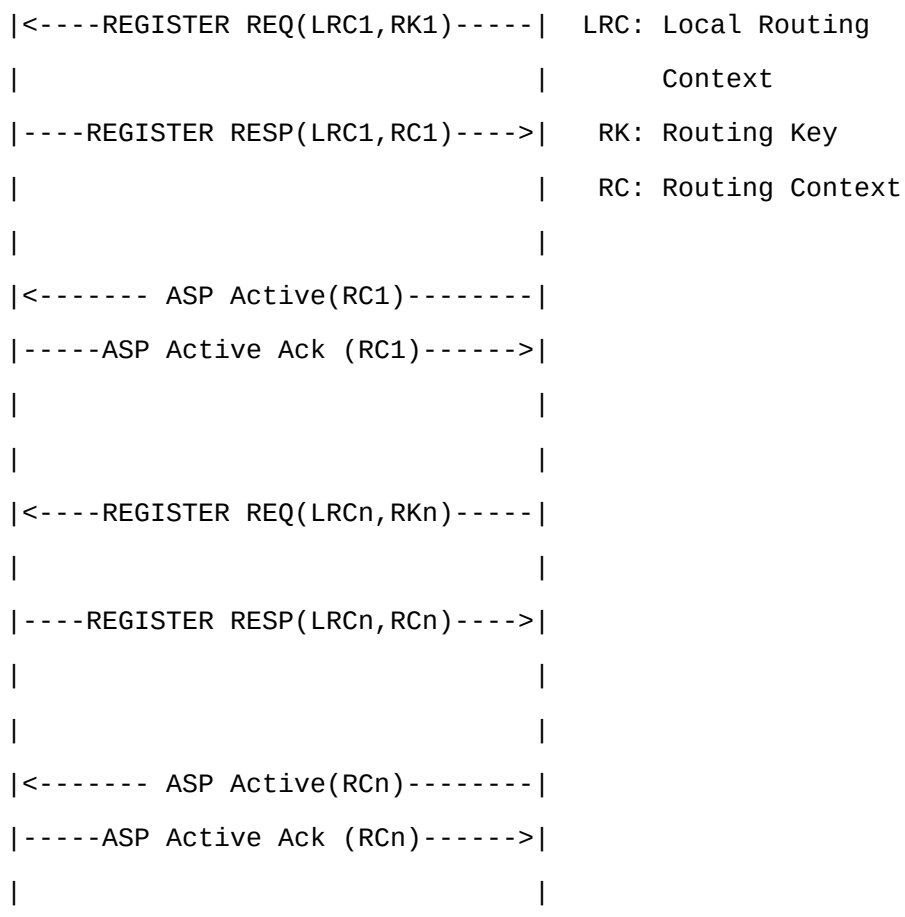
This scenario is the same as for 5.1.1.1 but with the optional exchange of registration information. In this case the Registration is accepted by the SGP.



Note: In the case of an unsuccessful registration attempt (e.g., Invalid RKn), the Register Response message will contain an unsuccessful indication and the ASP will not subsequently send an ASP Active message.

5.1.1.3 Single ASP in Multiple Application Servers (each with "1+0" sparing), Dynamic Registration (Case 1 û Multiple Registration Requests)



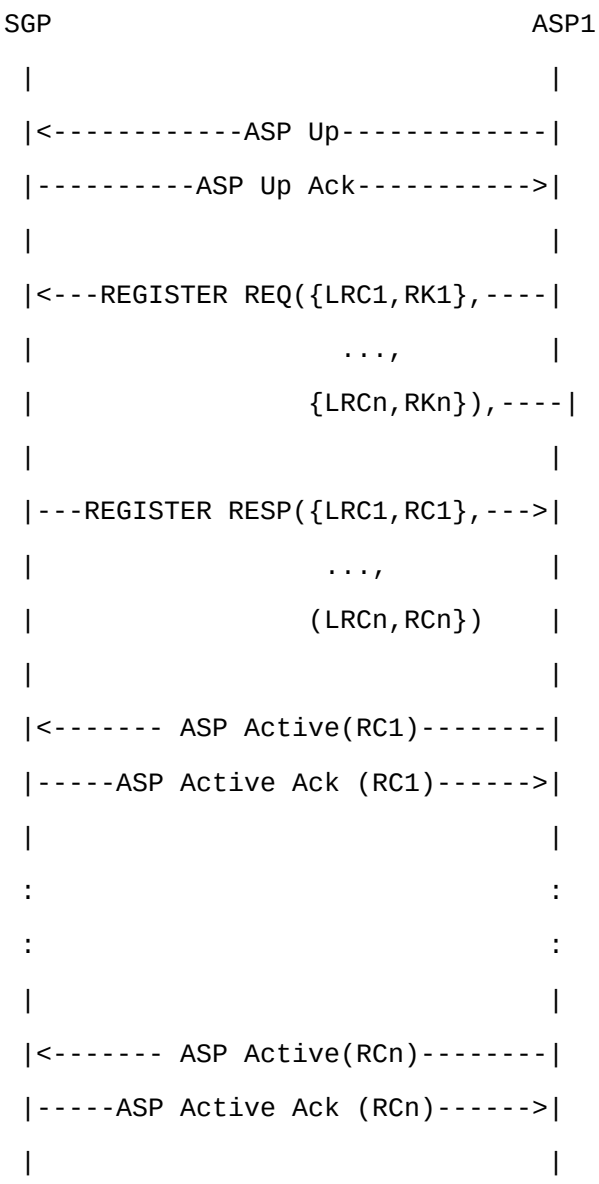


Note: In the case of an unsuccessful registration attempt (e.g., Invalid RKn), the Register Response message will contain an unsuccessful indication and the ASP will not subsequently send an ASP Active message. Each LRC/RK pair registration is considered independently.

It is not necessary to follow a Registration Request/Response message pair with an ASP Active message before sending the next Registration Request. The ASP Active message can be sent at any time after the related successful registration.

5.1.1.4 Single ASP in Multiple Application Servers (each with "1+0"

sparing), Dynamic Registration (Case 2 û Single Registration Request)

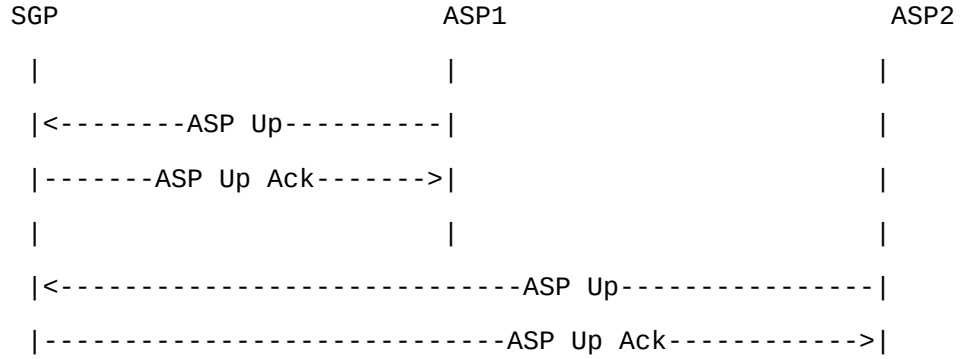


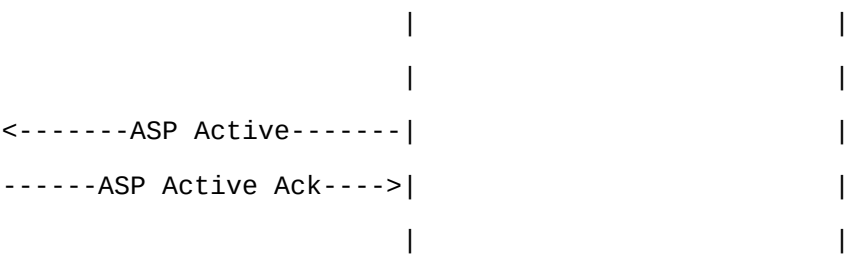
Note: In the case of an unsuccessful registration attempt (e.g., Invalid RKn), the Register Response message will contain an unsuccessful indication and the ASP will not subsequently send an ASP Active message. Each LRC/RK pair registration is considered independently.

The ASP Active message can be sent at any time after the related successful registration, and may have more than one RC.

5.1.2 Two ASPs in Application Server ("1+1" sparing)

This scenario shows the example M3UA message flows for the establishment of traffic between an SGP and two ASPs in the same Application Server, where ASP1 is configured to be in the ASP-ACTIVE state and ASP2 is to be a "back-up" in the event of communication failure or the withdrawal from service of ASP1. ASP2 may act as a hot, warm, or cold back-up depending on the extent to which ASP1 and ASP2 share call/transaction state or can communicate call state under failure/withdrawal events. The example message flow is the same whether the ASP Active messages indicate "Over-ride" or "Load-share" mode, although typically this example would use an Over-ride mode. The SGP MAY start sending any relevant DUNA, DRST and SCON messages to ASPs as soon as they enter the ASP-INACTIVE state. In the case of MTP Restart, the ASP-Active Ack message is only sent after all relevant DUNA/DRST/SCON messages have been transmitted to the concerned ASP.

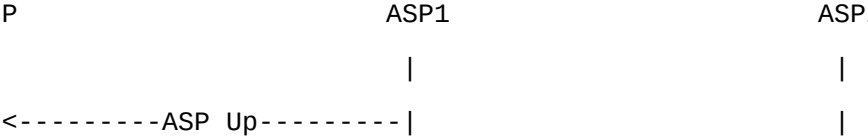


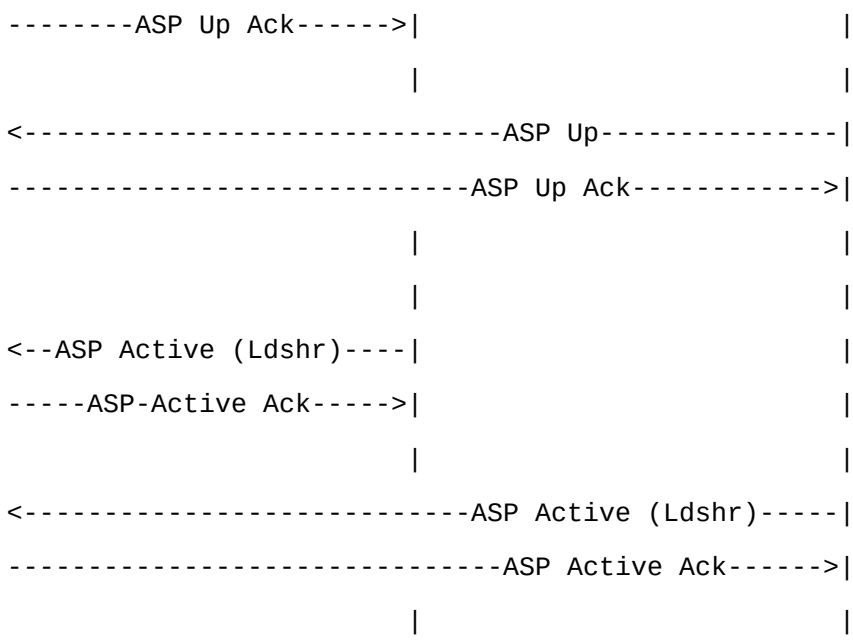


Note: It is also possible for ASP2 to send an ASP-Active ("Over-ride-Standby") message after ASP1 goes ASP-ACTIVE A similar sparing arrangement is created, except that the SGP may re-direct traffic to ASP2 more quickly in certain fail-over cases.

5.1.3 Two ASPs in an Application Server ("1+1" sparing, load-sharing case)

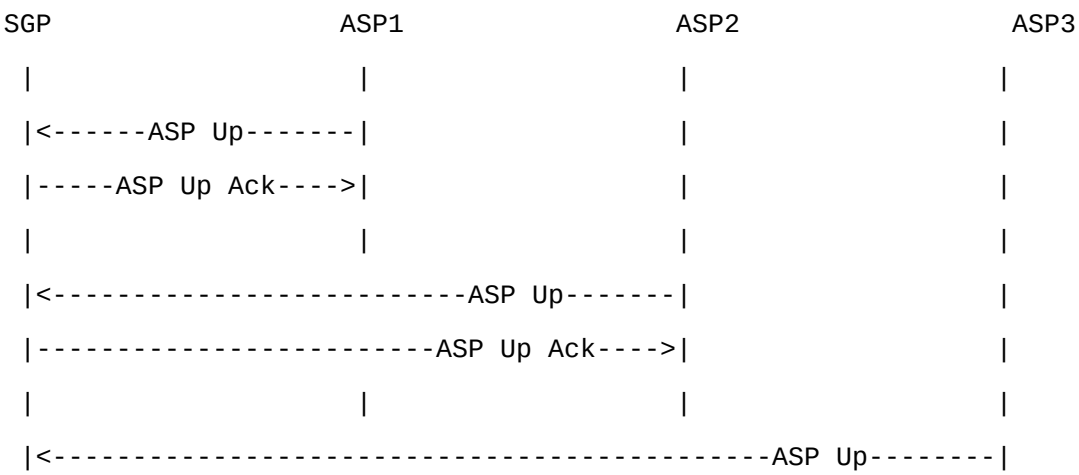
This scenario shows a similar case to Section 5.1.2 but where the two ASPs are brought to the state ASP-ACTIVE and subsequently load-share the traffic. In this case, one ASP is sufficient to handle the total traffic load. The sending of DUNA, DRST and SCON messages by the SGP is not shown but is similar to the case described in Section 5.1.2.

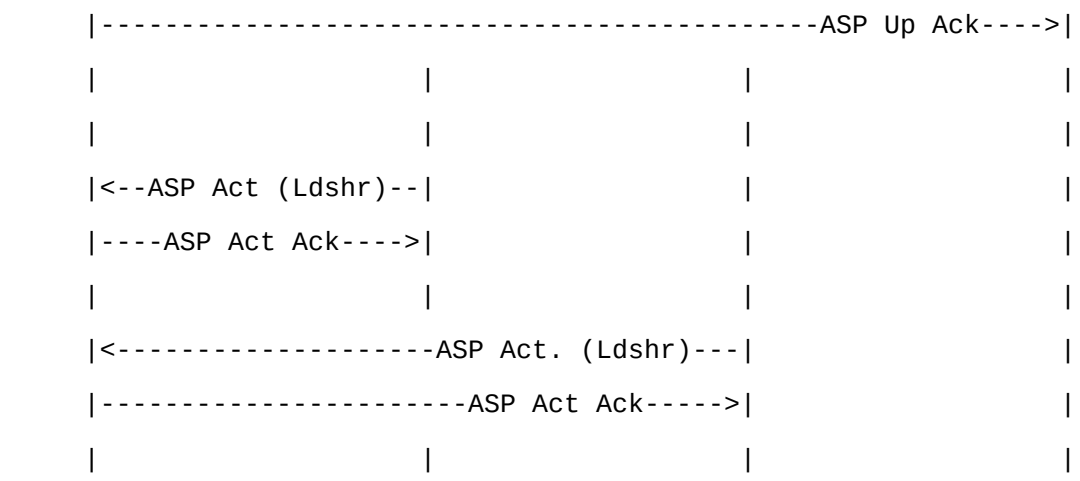




5.1.4 Three ASPs in an Application Server ("n+k" sparing, load-sharing case)

This scenario shows the example M3UA message flows for the establishment of traffic between an SGP and three ASPs in the same Application Server, where two of the ASPs are brought to the state ASP-ACTIVE and subsequently share the load. In this case, a minimum of two ASPs are required to handle the total traffic load (2+1 sparing). The sending of DUNA, DRST and SCON messages by the SGP is not shown but is similar to the case described in Section 5.1.2.





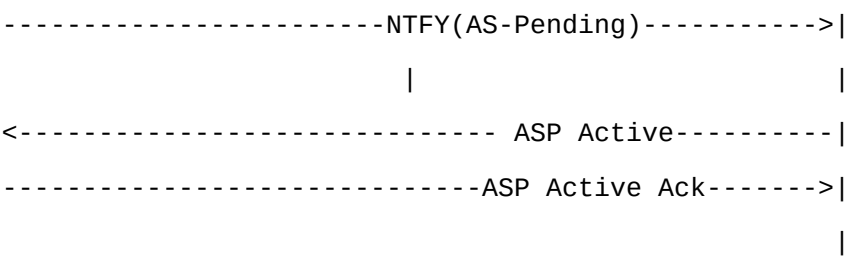
Note: It is also possible for ASP3 to send an ASP Active message ("Loadshare-Standby") after ASP1 and ASP2 go to the ASP-ACTIVE state A similar sparing arrangement is created, except that the SGP may redirect traffic to ASP3 more quickly in certain fail-over cases.

5.2 ASP Traffic Fail-over Examples

5.2.1 (1+1 Sparing, Withdrawal of ASP, Back-up Over-ride)

Following on from the example in Section 5.1.2, and ASP1 withdraws from service:

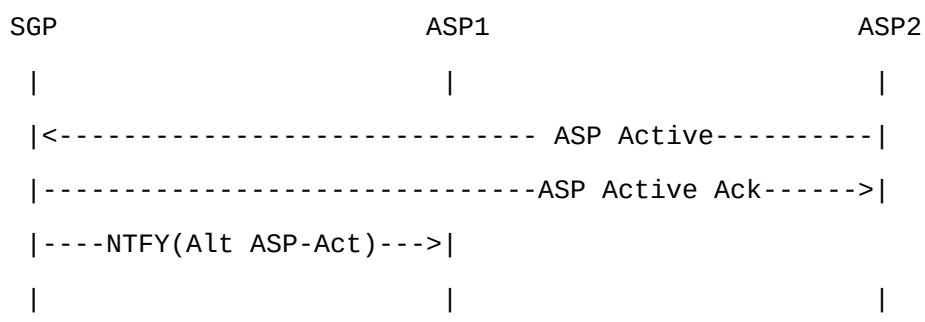




Note: If the SGP M3UA layer detects the loss of the M3UA peer (M3UA heartbeat loss or detection of SCTP failure), the initial ASP Inactive message exchange (i.e., SGP to ASP1) would not occur.

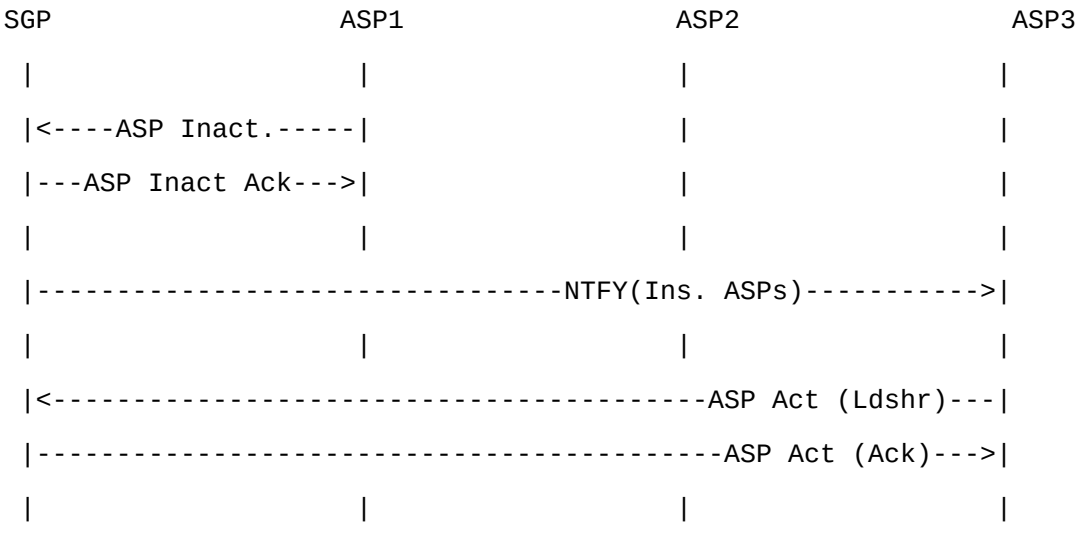
5.2.2 (1+1 Sparing, Back-up Over-ride)

Following on from the example in Section 5.1.2, and ASP2 wishes to over-ride ASP1 and take over the traffic:



5.2.3 (n+k Sparing, Load-sharing case, Withdrawal of ASP)

Following on from the example in Section 5.1.4, and ASP1 withdraws from service:

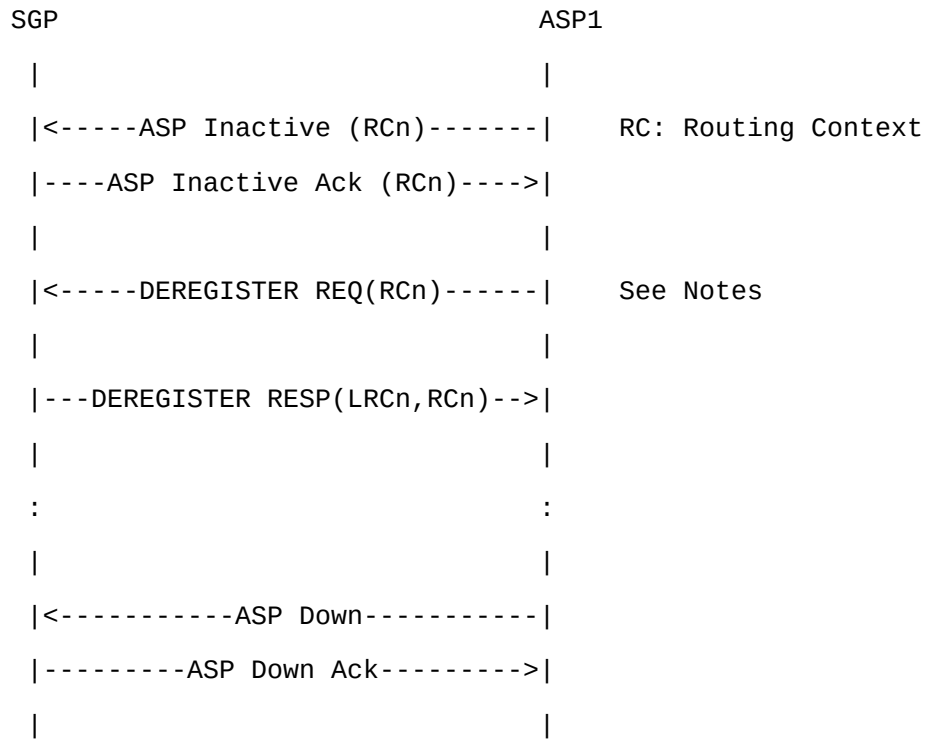


For the Notify message to be sent, the SG maintains knowledge of the minimum ASP resources required (e.g., if the SG knows that "n+k" = "2+1" for a load-share AS and "n" currently equals "1").

Note: If the SGP detects loss of the ASP1 M3UA peer (M3UA heartbeat loss or detection of SCTP failure), the initial ASP Inactive message exchange (i.e., SGP-ASP1) would not occur.

5.3 Normal Withdrawal of an ASP from an Application Server and Tear-down of an Association

An ASP which is now confirmed in the state ASP-INACTIVE (i.e., the ASP has received an ASP Inactive Ack message) may now proceed to the ASP-DOWN state, if it is to be removed from service. Following on from Section 5.2.1 or 5.2.3, where ASP1 has moved to the "Inactive" state:



Note: The Deregistration procedure MUST be used if the ASP previously used the Registration procedures for configuration within the Application Server. ASP Inactive and Deregister messages exchanges may contain multiple Routing Contexts.

The ASP SHOULD be ASP-INACTIVE and de-registered in all its Routing Contexts before attempting to move to the ASP-DOWN state.

5.4 M3UA/MTP3-User Boundary Examples

5.4.1 At an ASP

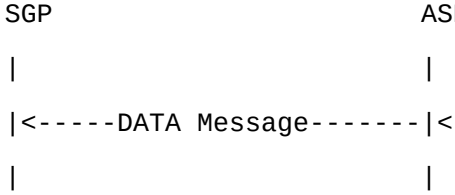
This section describes the primitive mapping between the MTP3 User and the M3UA layer at an ASP.

5.4.1.1 Support for MTP-TRANSFER Primitives at the ASP

5.4.1.1.1 Support for MTP-TRANSFER Request Primitive

When the MTP3-User on the ASP has data to send into the SS7 network, it uses the MTP-TRANSFER request primitive. The M3UA layer at the ASP will do the following when it receives an MTP-TRANSFER request primitive from the M3UA user:

- Determine the correct SGP;
- Determine the correct association to the chosen SGP;
- Determine the correct stream in the association (e.g., based on SLS);
- Determine whether to complete the optional fields of the DATA message;
- Map the MTP-TRANSFER request primitive into the Protocol Data field of a DATA message;
- Send the DATA message to the remote M3UA peer at the SGP, over the SCTP association.



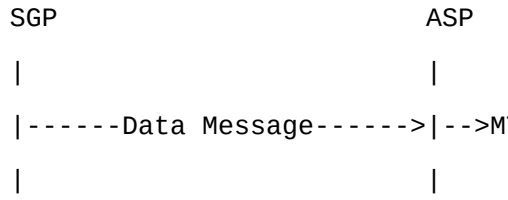
5.4.1.1.2 Support for the MTPûTRANSFER Indication Primitive

When the M3UA layer on the ASP receives a DATA message from the remote M3UA peer at the SGP, it will do the following:

- Evaluate the optional fields of the DATA message, if present;

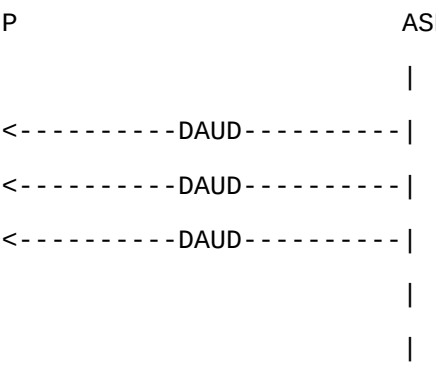
- Map the Protocol Data field of a DATA message into the MTP-TRANSFER indication primitive;

- Pass the MTP-TRANSFER indication primitive to the user part. In case of multiple user parts, the optional fields of the Data message are used to determine the concerned user part.



5.4.1.1.3 Support for ASP Querying of SS7 Destination States

There are situations such as temporary loss of connectivity to the SGP that may cause the M3UA layer at the ASP to audit SS7 destination availability/congestion states. Note: there is no primitive for the MTP3-User to request this audit from the M3UA layer as this is initiated by an internal M3UA management function.



5.4.2 At an SGP

This section describes the primitive mapping between the MTP3-User and the M3UA layer at an SGP.

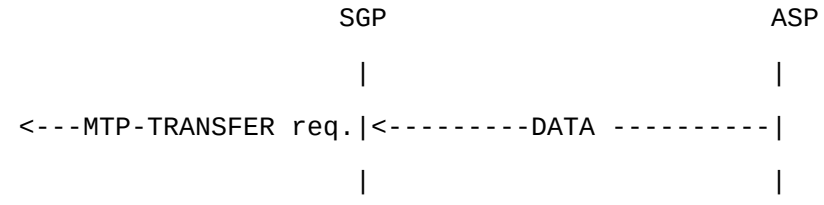
5.4.2.1 Support for MTP-TRANSFER Request Primitive at the SGP

When the M3UA layer at the SGP has received DATA messages from its peer destined to the SS7 network it will do the following:

- Evaluate the optional fields of the DATA message, if present, to determine the Network Appearance;

- Map the Protocol data field of the DATA message into an MTP-TRANSFER request primitive;

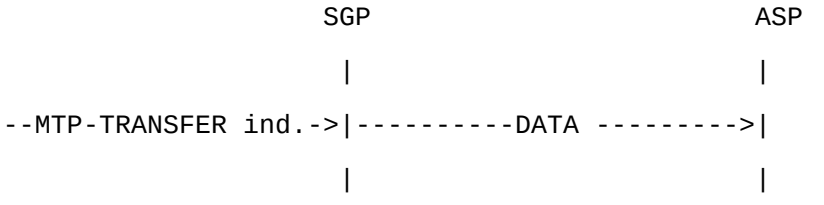
- Pass the MTP-TRANSFER request primitive to the MTP3 of the concerned Network Appearance.



5.4.2.2 Support for MTP-TRANSFER Indication Primitive at the SGP

When the MTP3 layer at the SGP has data to pass its user parts, it will use the MTP-TRANSFER indication primitive. The M3UA layer at the SGP will do the following when it receives an MTP-TRANSFER indication primitive:

- Determine the correct ASP;
- Determine the correct association to the chosen ASP;
- Determine the correct stream in the association (e.g., based on SLS);
- Determine whether to complete the optional fields of the DATA message;
- Map the MTP-TRANSFER indication primitive into the Protocol Data field of a DATA message;
- Send the DATA message to the remote M3UA peer in the ASP, over the SCTP association

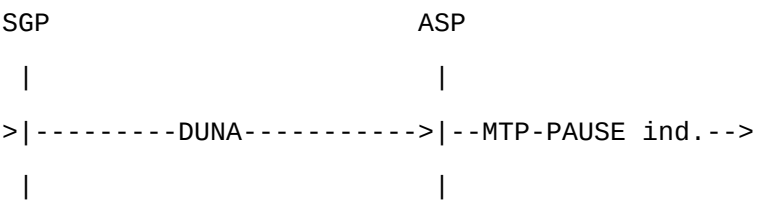


5.4.2.3 Support for MTP-PAUSE, MTP-RESUME, MTP-STATUS Indication Primitives

The MTP-PAUSE, MTP-RESUME and MTP-STATUS indication primitives from the MTP3 upper layer interface at the SGP need to be made available to the remote MTP3 User Part lower layer interface at the concerned ASP(s).

5.4.2.3.1 Destination Unavailable

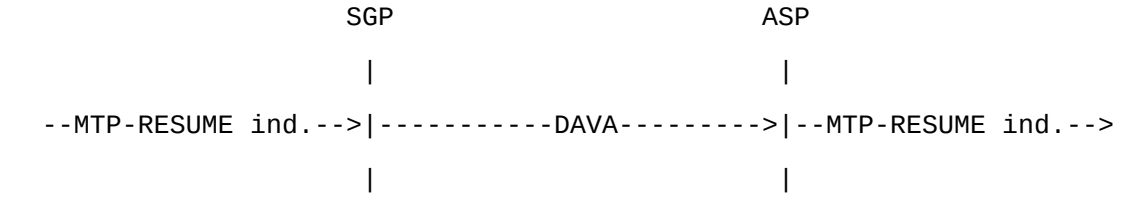
The MTP3 layer at the SGP will generate an MTP-PAUSE indication primitive when it determines locally that an SS7 destination is unreachable. The M3UA layer will map this primitive to a DUNA message. The SGP M3UA layer determines the set of concerned ASPs to be informed based on internal SS7 network information associated with the MTP-PAUSE indication primitive indication.



5.4.2.3.2 Destination Available

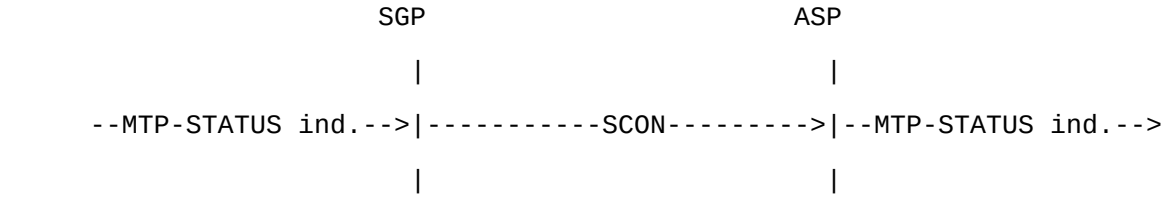
The MTP3 at the SGP will generate an MTP-RESUME indication primitive when it determines locally that an SS7 destination that was previously unreachable is now reachable. The M3UA layer will map this primitive

to a DAVA message. The SGP M3UA determines the set of concerned ASPs to be informed based on internal SS7 network information associated with the MTP-RESUME indication primitive.



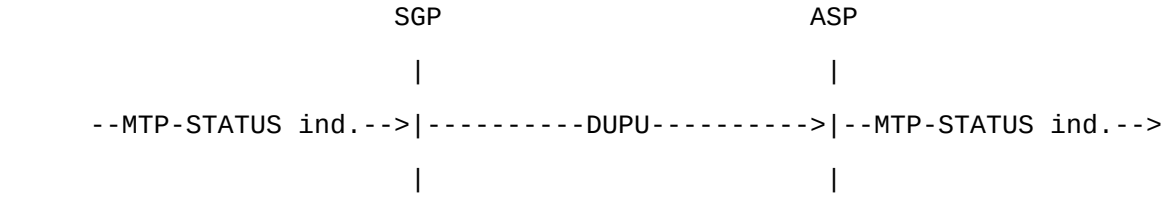
5.4.2.3.3 SS7 Network Congestion

The MTP3 layer at the SGP will generate an MTP-STATUS indication primitive when it determines locally that the route to an SS7 destination is congested. The M3UA layer will map this primitive to a SCON message. It will determine which ASP(s) to send the SCON message to, based on the intended Application Server.



5.4.2.3.4 Destination User Part Unavailable

The MTP3 layer at the SGP will generate an MTP-STATUS indication primitive when it receives an UPU message from the SS7 network. The M3UA layer will map this primitive to a DUPU message. It will determine which ASP(s) to send the DUPU based on the intended Application Server.



6. Security

6.1 Introduction

M3UA is designed to carry signalling messages for telephony services. As such, M3UA must involve the security needs of several parties: the end users of the services; the network providers and the applications involved. Additional requirements may come from local regulation. While having some overlapping security needs, any security solution should fulfil all of the different parties' needs.

6.2 Threats

There is no quick fix, one-size-fits-all solution for security. As a transport protocol, M3UA has the following security objectives:

* Availability of reliable and timely user data transport.
* Integrity of user data transport.
* Confidentiality of user data.

M3UA is recommended to be transported on SCTP. SCTP [13] provides certain transport related security features, such as some protection against:

* Blind Denial of Service Attacks
* Flooding
* Masquerade
* Improper Monopolization of Services

When M3UA is running in professionally managed corporate or service provider network, it is reasonable to expect that this network includes an appropriate security policy framework. The "Site Security Handbook" [21] should be consulted for guidance.

When the network in which M3UA runs in involves more than one party, it may not be reasonable to expect that all parties have implemented security in a sufficient manner. In such a case, it is recommended that IPSEC is used to ensure confidentiality of user payload. Consult [22] for more information on configuring IPSEC services.

6.3 Protecting Confidentiality

Particularly for mobile users, the requirement for confidentiality may include the masking of IP addresses and ports. In this case application level encryption is not sufficient; IPSEC ESP [23] SHOULD be used instead. Regardless of which level performs the encryption, the IPSEC ISAKMP [24] service SHOULD be used for key management.

7. IANA Considerations

7.1 SCTP Payload Protocol Identifier

IANA has assigned an M3UA value for the Payload Protocol Identifier in the SCTP DATA chunk. The following SCTP Payload Protocol Identifier is registered:

M3UA "3"

The SCTP Payload Protocol Identifier value "3" SHOULD be included in each SCTP DATA chunk, to indicate that the SCTP is carrying the M3UA protocol. The value "0" (unspecified) is also allowed but any other values MUST not be used. This Payload Protocol Identifier is not directly used by SCTP but MAY be used by certain network entities to identify the type of information being carried in a DATA chunk.

The User Adaptation peer MAY use the Payload Protocol Identifier as a way of determining additional information about the data being presented to it by SCTP.

7.2 M3UA Port Number

IANA has registered SCTP (and UDP/TCP) Port Number 2905 for M3UA.

7.3 M3UA Protocol Extensions

This protocol may also be extended through IANA in three ways:
-- through definition of additional message classes,
-- through definition of additional message types, and
-- through definition of additional message parameters

The definition and use of new message classes, types and parameters is an integral part of SIGTRAN adaptation layers. Thus these extensions are assigned by IANA through an IETF Consensus action as defined in Guidelines for Writing an IANA Considerations Section in RFCs (25]

The proposed extension must in no way adversely affect the general working of the protocol.

7.3.1 IETF Defined Message Classes

The documentation for a new message class MUST include the following information:

(a) A long and short name for the new message class;

(b) A detailed description of the purpose of the message class.

7.3.2 IETF Defined Message Types

The documentation for a new message type MUST include the following information:

(a) A long and short name for the new message type;

(b) A detailed description of the structure of the message;.

(c) A detailed definition and description of intended use for each field within the message;

(d) A detailed procedural description of the use of the new message type within the operation of the protocol;

(e) A detailed description of error conditions when receiving this message type.

When an implementation receives a message type which it does not support, it MUST respond with an Error (ERR) message ("Unsupported Message Type").

7.3.3 IETF Defined Parameter Extension

Documentation of the message parameter MUST contain the following information:

(a) Name of the parameter type;
(b) Detailed description of the structure of the parameter field. This structure MUST conform to the general type-length-value format described in Section 3.2;
(c) Detailed definition of each component of the parameter value;
(d) Detailed description of the intended use of this parameter type, and an indication of whether and under what circumstances multiple instances of this parameter type may be found within the same message.

8. Acknowledgements

The authors would like to thank Antonio Roque Alvarez, Joyce Archibald, Tolga Asveren, Brian Bidulock, Dan Brendes, Nikhil Jain, Joe Keller, Kurt Kite, Ming Lin, Steve Lorusso, John Loughney, Naoto Makinae, Howard May, Barry Nagelberg, Neil Olson, Heinz Prantner, Shyamal Prasad, Mukesh Punhani, Selvam Rengasami, Ray Singh, Michael Tuexen, Nitin Tomar, Gery Verwimp, Kazuo Watanabe, Ben Wilson and many others for their valuable comments and suggestions.

9. References

[1] RFC 2719, "Framework Architecture for Signaling Transport", L. Ong et al, October 1999

[2] ITU-T Recommendations Q.761 to Q.767, "Signalling System No.7 (SS7) - ISDN User Part (ISUP)"

[3] ANSI T1.113 û "Signaling System Number 7 - ISDN User Part"

[4] ETSI ETS 300 356-1 "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 2 for the international interface; Part 1: Basic services"

[5] ITU-T Recommendations Q.711 to Q.715, "Signalling System No. 7 (SS7) - Signalling Connection Control Part (SCCP)"

[6] ANSI T1.112 "Signaling System Number 7 - Signaling Connection Control Part"

[7] ETSI ETS 300 009-1, "Integrated Services Digital Network (ISDN); Signalling System No.7; Signalling Connection Control Part (SCCP) (connectionless and connection-oriented class 2) to support international interconnection; Part 1: Protocol specification"

[8] ITU-T Recommendation Q.720, "Telephone User Part"

[9] ITU-T Recommendations Q.771 to Q.775 "Signalling System No. 7 (SS7) - Transaction Capabilities (TCAP)"

[10] ANSI T1.114 "Signaling System Number 7 - Transaction Capabilities Application Part"

[11] ETSI ETS 300 287-1, "Integrated Services Digital Network (ISDN); Signalling System No.7; Transaction Capabilities (TC) version 2; Part 1: Protocol specification"

[12] 3G TS 25.410 V4.0.0 (2001-04) "Technical Specification - 3rd Generation partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu Interface: General Aspects and Principles"

[13] RFC 2960, "Stream Control Transport Protocol", R. Stewart et al, October 2000.

[14] ITU-T Recommendations Q.701 to Q.705, "Signalling System No. 7 (SS7) - Message Transfer Part (MTP)"

[15] ANSI T1.111 "Signaling System Number 7 - Message Transfer Part"

[16] ETSI ETS 300 008-1, "Integrated Services Digital Network (ISDN); Signalling System No.7; Message Transfer Part (MTP) to support international interconnection; Part 1: Protocol specification"

[17] ITU-T Recommendation Q.2140 "B-ISDN ATM Adaptation Layer - Service Specific Coordination Function for signalling at the Network Node Interface (SSCF at NNI)"

[18] ITU-T Recommendation Q.2110 "B-ISDN ATM Adaptation Layer - Service Specific Connection Oriented Protocol (SSCOP)"

[19] RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997.

[20] ITU-T Recommendation Q.2210 "Message Transfer Part Level 3 functions and messages using the services of ITU Recommendation

Q.2140"

[21] RFC 2196, "Site Security Handbook", B. Fraser Ed., September 1997

[22] RFC 2401, "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998.

[23] RFC 2406, "IP Encapsulating Security Payload (ESP)", S.Kent and R. Atkinson, November 1998.

[24] RFC 2408, "Internet Security Association and Key Management Protocol", D. Maughan, M. Schertler, M. Schneider and J. Turner, November 1998.

[25] RFC 2434, "Guidelines for Writing an IANA Considerations Section in RFCs", T. Narten and H. Alvestrand, October 1998

10. Bibliography

[26] <draft-ietf-sigtran-m2ua-07.txt>, "MTP2-User Adaptation Layer", K. Morneault et al, February 2001 (Work in Progress)

11. Author's Addresses

Greg Sidebottom
Kanata, Ontario, Canada
gregside@home.com

Guy Mousseau
Nortel Networks
3685 Richmond Rd
Nepean, Ontario, Canada K2H 5B7

Lyndon Ong
Ciena
10480 Ridgeview Court
Cupertino, CA 95014
lyong@ciena.com

Ian Rytina
Ericsson Australia
37/360 Elizabeth Street
Melbourne, Victoria 3000, Australia
ian.rytina@ericsson.com.au

Hanns Juergen Schwarzbauer
SIEMENS AG
Hofmannstr. 51
81359 Munich, Germany
HannsJuergen.Schwarzbauer@icn.siemens.de

Klaus D. Gradischnig
NeuStar, Inc
1120 Vermont Ave. N.W.Suite 400
Washington D.C 20005
klaus.gradischnig@neustar.com

Ken Morneault
Cisco Systems Inc.
13615 Dulles Technology Drive
Herndon, VA, USA 20171

EMail: kmorneau@cisco.com

Malleswar Kalla

Telcordia Technologies

MCC 1J211R

445 South Street

Morristown, NJ, USA 07960

Email: kalla@research.telcordia.com

Normand Glaude

Performance Technologies

150 Metcalf Sreet, Suite 1300

Ottawa, Ontario, Canada K2P 1P1

EMail: nglaude@microlegend.com

This draft expires December 2001.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
February 2001					Initial draft	0.0.1	0.0.2
February 2001					Second draft	0.0.2	0.1.0
February 2001					Contributions and comments from TSG-CN WG4#6.1 Madrid Ad Hoc incorporated	0.1.0	0.2.0
February 2001					Contributions and comments from TSG-CN WG4#6.1 Madrid Ad Hoc incorporated and draft further elaborated	0.2.0	2.0.0
March 2001					Comments from TSG-CN WG4#7 incorporated.	2.0.0	2.1.0
March 2001	CN#11	NP-010079			Annex A: M3UA updated to the latest available version 6 Approved in CN#11	2.1.0	4.0.0
May 2001					 Foreword added	4.0.0	4.0.1
Sep 2001	CN#13	NP-010452	001		Change of M 3UA version	4.0.1	4.1.0
Sep 2001	CN#13				Editorial clean up	4.0.1	4.1.0
Jun 2002	CN#16				Corrupted Figure 5.3/1 fixed	4.1.0	4.1.1

History

Document history		
V4.0.1	May 2001	Publication
V4.1.0	September 2001	Publication (Withdrawn)
V4.1.1	June 2002	Publication